BILLIN

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID DoD-2022-OS-0139]

Privacy Act of 1974; System of Records

AGENCY: Department of Defense (DoD).

ACTION: Notice of a new system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the DoD is establishing a new Department-wide system of records titled, "Enterprise Identity, Credential, and Access Management (ICAM) Records, DoD-0015." This system of records will support the management of individual identity information, support the provision of credentials to individuals and entities to provide them access to the DoD information services and data they require, and support a standardized DoD-wide process and protocol for individual system and data access across the enterprise to improve security and cost savings.

DATES: This system of records is effective upon publication; however, comments on the Routine Uses will be accepted on or before [INSERT 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 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: Ms. Rahwa Keleta, Defense Privacy and Civil Liberties Division, Directorate for Privacy, Civil Liberties and Freedom of Information, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Department of Defense, 4800 Mark Center Drive, Mailbox #24, Suite 08D09, Alexandria, VA 22350-1700; OSD.DPCLTD@mail.mil; (703) 571-0070.

SUPPLEMENTARY INFORMATION:

I. Background

DoD is establishing the Enterprise Identity, Credentialing, and Access Management (ICAM) Records, DoD-0015, as a DoD-wide Privacy Act system of records. A DoD-wide system of records notice (SORN) supports multiple DoD paper or electronic recordkeeping systems operated by more than one DoD component that maintain the same kind of information about individuals for the same purpose. Establishment of DoD-wide SORNs helps DoD standardize the rules governing the collection, maintenance, use, and sharing of personal information in key areas across the enterprise. DoD-wide SORNs also reduce duplicative and overlapping SORNs published by separate DoD components. The creation of DoD-wide SORNs is expected to make locating relevant SORNs easier for DoD personnel and the public, and create efficiencies in the operation of the DoD privacy program.

This system of records covers the Department's maintenance of records about individual users of the DoD network and information systems, to create a secure and trusted environment where users can access authorized resources, including services, information systems, and data, thereby supporting mission accomplishment while efficiently providing oversight of DoD users

on the network. There are significant advantages in providing ICAM services at the enterprise level, including efficiencies in consolidating network services; improved security; cost savings; and enabling the creation of digital identities for a single individual for use across the enterprise. The purposes of this system of records include maintaining standardized user access controls, which provides for supporting users through self-service functions, and ensuring only approved users may access systems and data across the DoD enterprise. ICAM more efficiently reinforces the rules and controls governing the collection, maintenance, use, and sharing of information. This SORN will reduce duplicative efforts and overlap from SORNs published by separate DoD Components for solutions pursuing the same functions.

DoD SORNs 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 FOIA Directorate website at https://dpcld.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 particulars 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, DoD has provided a report of this system of records to the OMB and to Congress.

Dated: December 10, 2022.

Aaron T. Siegel,

Alternate OSD Federal Register

Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER: Enterprise Identity, Credential, and Access Management (ICAM) Records, DoD-0015.

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): Chief Information Officer, Department of Defense, 6000 Defense Pentagon, Washington, DC 20301–6000; osd.pentagon.dod-cio.list.cio@mail.mil; 703-614-7323.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. 2222, Defense Business Systems: Business Process Reengineering; Enterprise Architecture; Management; 10 U.S.C. 2224, Defense Information Assurance Program; 10 U.S.C. Chapter 8-Defense Agencies and Department of Defense Field Activities; 31 U.S.C. 902, Authority and functions of agency Chief Financial Officers; Homeland Security Presidential Directive (HSPD) 12, Policies for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; OMB M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management; National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors; DoD Instruction 8320.02, Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense; DoD Instruction 8320.07, Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense; and DoD Instruction 8520.03, Identity Authentication for Information Systems.

PURPOSE(S) OF THE SYSTEM: This system of records supports the Department's maintenance of records about individual users of the DoD network and information systems, to create a secure and trusted environment where users can access authorized resources, including services, information systems, and data. ICAM more efficiently reinforces the rules and controls governing the collection, maintenance, use, and sharing of information and supports the standardization of user access controls, self-service functions, and ensuring that only approved users access systems and data across the DoD enterprise. The system creates a single user record, consolidating all pertinent data associated with the individual under one account. The principal purpose of the ICAM system is to capture and maintain a record of names, digital signatures, approved access, and other identifiers from authoritative sources to provide and maintain a record of access management to DoD systems and resources, to include Financial Management and Reporting Records and Information Systems Security records. This information is used to provide the following ICAM services:

A. Enables and manages the digital flow of identity, credential, and access-management data for DoD-affiliated individuals.

B. Provides authentication to DoD networks and resources through common standards, shared services, and federation.

C. Facilitates managed access to protected resources, such as federally managed facilities, information systems, and data.

D. Scopes access that is necessary and relevant to authorize the actions each user is allowed to perform on a given system; provides audit capability to ensure proper access is granted.

E. Supports aligning existing account or entitlement information from DoD authoritative source systems to consuming applications.

F. Provides fast, reliable, secure, and auditable capabilities across the DoD enterprise in a manner enhancing user experience and supports the critical missions.

G. Provides consistent auditing capabilities such as monitoring and logging to support identity analytics for detecting insider threats and external attacks.

H. Enables the determination of requirements for identification, credentialing, authentication, and authorization lifecycle management for future planning and fiscal management.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Individuals who have been issued credentials for access to DoD data, systems, or facilities which may include uniformed services personnel, including National Guard and Reserve components; former members and retirees of the uniformed services; dependent family members of uniformed services members; civilian employees, contractors, and any other DoD-"affiliated" individuals requiring or requesting access to DoD or DoD-controlled information systems and/or DoD- or DoD contractor-operated, controlled, or secured facilities.

CATEGORIES OF RECORDS IN THE SYSTEM:

A. Personal information, such as name, DoD Identification (ID) Number, or other DoD-assigned student or educational ID number, date and place of birth, gender, citizenship, mother's middle/maiden name, driver's license, passport information, photograph, email address(es), personal and duty phone numbers, emergency contact information, race and ethnic origin.

B. Employment-related information, such as employment status, duty position, service component, branch, personnel classification, security clearance, grade/rank/series, military status, military occupational specialty, official orders, unit of assignment, occupation, access rights provisioned in DoD systems and applications, DD Form 577, "Appointment/Termination Record – Authorized Signature," financial position appointed to, and other organizational affiliation information.

C. Course and training data, such as examination and course completion status.

RECORD SOURCE CATEGORIES:

A. Individuals.

B. All DoD databases flowing into or accessed through the following integrated data systems, environments, applications, and tools, including:

Defense Finance and Accounting Services financial business feeder systems, Procurement Integrated Enterprise Environment, Defense Manpower Data Center including the Defense Eligibility Enrollment System (DEERS), 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 Operational Data System, Force Risk Reduction, Medical Readiness Reporting System, Medical Health System Data Repository, National Guard Bureau Human/Personnel, Resource, and Manpower Systems, National Guard Bureau System, and commensurate data from DoD Component systems performing ICAM services.

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 of 1987, as amended.

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 paper in secure facilities in a locked drawer behind a locked door. Electronic records may be stored locally on 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 individual name, DoD ID Number, or email address.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

A. Financial Records: The DD Form 577 records are retained for six (6) years after the final invoice or Intra-Government Payment and Collection or other similar documentation and then destroyed (DAA-GRS2013-0003-0001).

B. General System Records: Records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users. These records are temporary and will be destroyed in accordance with NARA guidance, when business use ceases (DAA-GRS-2013-0006-0003).

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: 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, DoD has established security audit and accountability policies and procedures which support the safeguarding of PII and detection of potential PII incidents. 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 follow the procedures in 32 CFR part 310. Individuals should address written inquiries to the DoD component with oversight of the records, as the component has Privacy Act responsibilities concerning access, amendment, and disclosure of the records within this system of records. The public may identify the contact information for the appropriate DoD office through the following website: www.FOIA.gov. Signed written requests should contain the name and number of this system of records notice along with the full name, current address, telephone number and email address of the individual along with the name and number of this system of records notice. 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: Individuals seeking to amend or correct the content of records about them should follow the procedures in 32 CFR part 310.

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: None

[FR Doc. 2022-27356 Filed: 12/15/2022 8:45 am; Publication Date: 12/16/2022]