This document is scheduled to be published in the Federal Register on 08/10/2021 and available online at **federalregister.gov/d/2021-17000**, and on **govinfo.gov**

BILLING C

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2021-OS-0083]

Privacy Act of 1974; System of Records

AGENCY: Defense Information Systems Agency (DISA), 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 Enterprise Application and Services Forest (EASF), K890.15. This system of records was originally established by the DISA to collect and maintain records on the core active directory (AD) Infrastructure (domain controllers) for Enterprise Services such as DoD Enterprise Email (DEE), Identity Synchronization Services (IdSS), and DoD Enterprise Portal Service (DEPS). It is an Enterprise-wide hierarchical directory structure designed to employ greater centralization and standardization of network management for user data, security, and distributed resources and services across the DoD Enterprise. This system of records notice (SORN) is being updated to make various compliance changes as well as add DoD's standard routine uses.

DATES: This 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: DoD cannot receive written comments at this time due to the COVID-19 pandemic.

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: Mrs. Jeanette M. Weathers-Jenkins, DISA Privacy Officer, 6914 Cooper Ave, Fort Meade, MD 20755-7090, or by phone at (301) 225-8158.

SUPPLEMENTARY INFORMATION:

I. Background

The DISA is modifying the K890.15 EASF system of records to allow the provision of user accounts, and to authenticate users to DoD enterprise Web applications (e.g., Defense Collaboration Services, Defense Enterprise Portal, DEE) for non-dual persona personnel with DoD's Personal Identity Verification (PIV) - Authentication (Auth) certificate, rather than DoD's E-mail signing certificate. Subject to public comment, the DoD proposes to update this SORN to add the standard DoD routine uses (routine uses A through I) and to allow for additional disclosures outside DoD related to the purpose of this system of records. Additionally, the following sections of this SORN are being modified as follows: (1) to the Authority for Maintenance of the System section to update citation(s) and add additional authorities; (2) purpose of the system to improve clarity; (3) to the Categories of Individuals Covered by the System section to expand the individuals covered and Categories of Records to clarify how the records relate to the revised Category of Individuals; (4) Record Source Categories to account for Five Eyes partners and Coalition partners exchange in order to populate the information into the Five Eyes national directory; (5) Routine Uses to align with DoD's standard routine uses; (6) to the Administrative, Technical, and Physical Safeguards to update the individual safeguards

protecting the personal information; (7) to the Record Access Procedures section to reflect the need for individuals to identify the appropriate DoD office or component to which their request should be directed; and (8) to the Contesting Records Procedures and Notification procedures section 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 Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD) 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, DPCLTD has provided a report of this system of records to the OMB and to Congress.

Dated: August 5, 2021.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer,

Department of Defense.

SYSTEM NAME AND NUMBER: Enterprise Application and Services Forest (EASF), K890.15

SYSTEM CLASSIFICATION: Unclassified.

SYSTEM LOCATION: System locations may be obtained from the system manager.

SYSTEM MANAGER(S): Chief, Enterprise Directory Services Section, Defense Information Systems Agency (DISA), Services Directorate, Applications Division, Infrastructure Applications Branch, 6910 Cooper Ave., Fort Meade, MD 20755-7090, telephone number 301-225-9201, email: disa.meade.se.list.idss-product-management@mail.mil.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. Chapter 8, Defense Agencies and Department of Defense Field Activities; DoD Directive 5105.19, Defense Information Systems Agency (DISA); DoD Instruction (DoDI) 1000.25, DoD Personnel Identity Protection (PIP) Program; DoDI 5200.46, DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC); and DoDI 8520.03, Identity Authentication for Information Systems.

PURPOSE(S) OF THE SYSTEM: This system of records provides the core active directory (AD) Infrastructure (domain controllers) for Enterprise Services such as DoD Enterprise Email (DEE), Identity Synchronization Services (IdSS), and DoD Enterprise Portal Service (DEPS). It also:

A. Supports the provision of user accounts and authenticates users to DoD enterprise Web applications (e.g., Defense Collaboration Services, Defense Enterprise Portal, DEE) for non-dual personal personnel with DoD's Personal Identity Verification (PIV) - Authentication (Auth) certificate;

B. Provides an Enterprise-wide hierarchical directory structure designed to employ greater centralization and standardization of network management for user data, security, and distributed resources and services across the DoD Enterprise; and

C. Supports the use of enterprise services to establish a reliable and uniform secure data portal for the transmittal of shared information between DoD and VA.

D. To support continuous data exchange between DoD and its Coalition Partners to enable current and future information sharing capabilities that are used by the respective warfighters for conducting mission supporting operations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

A. DoD personnel, meaning those who have been issued DoD CAC or a DoD Class 3 Public Key Infrastructure (PKI) certificate to include civilian employees, military personnel, contractors, and other individuals detailed or assigned to DoD Components.

B. Department of Veterans Affairs (VA) PIV card holders identified by the VA's Interagency Care Coordination Committee (IC3).

CATEGORIES OF RECORDS IN THE SYSTEM:

A. For DoD personnel: Individuals name, unique identifiers including DoD ID number, other unique identifier, Federal Agency Smart Credential Number (FASC-N), login name, legacy login name, and persona username, object class, rank, title, job title, persona type code (PTC), persona display name (PDN), address, email, phone, and other contact information for work and home locations, US government agency code, service code, personnel category code, non-US government agency object common name, user account control, information technology service entitlements, Unit Identification Code (UIC), and PKI certificate information, Administrative Organization Code, DoD component, DoD sub-component, Non-DoD agency, Directory publishing restrictions, Reserve Component Code, Billet Code, Pay Grade, type of investigation, date of investigation, and security clearance level.

B. For VA personnel: Individual's name, other unique identifier, primary and other work e-mail addresses, administrative organization code, duty sub-organization code persona e-mail address, e-mail encryption certificate, driver's license number.

NOTE: This system does not collect or maintain the individual's Social Security Number.

RECORD SOURCE CATEGORIES: Records and information stored in this system of records are obtained from: Defense Manpower Data Center (DMDC)'s Defense Eligibility Enrollment Reporting System (DEERS), Person Data Repository (PDR) for DoD person and person data, the DISA DoD PKI Global Directory Service (GDS) for users with PKI email certificates, Five Eyes partners, and the Coalition partners.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE 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 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 such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

J. To the United States Coast Guard (USCG) to share DoD information to ensure it maintains a state of readiness to function as a specialized military Service in the Department of Navy in a time of war or national emergency.

K. To DoD-approved Coalition Partners for the purposes of routine mission supporting activities. In return, the Coalition partner may disclose system of records information to DoD or a DoD component.

L. To partner Five Eyes (FVEY) Nations to provide information pursuant to existing bilateral agreement(s) in order to populate the information into the FVEY national directory.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records may be stored electronically in secure facilities 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: These records are retrieved by individual name and DoD ID Number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: System's sole function is to receive and integrate data from two or more other systems and export the resultant product to yet another independent system. These records are maintained as temporary which may be destroyed upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Access to the type and amount of data is governed by privilege management software and policies developed and enforced by Federal government personnel. Data is protected by repository and interfaces, including, but not limited to multi-layered firewalls, Secure Sockets Layer/Transport Layer Security (SSL/TLS) connections, access control lists, file system permissions, intrusion detection and prevention systems and log monitoring. Complete access to all records is restricted to and controlled by certified system management personnel, who are responsible for maintaining the EASF directory integrity and the data confidentiality. Access to computerized data is restricted by CAC.

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 Defense Information Systems Agency (DISA), FOIA Service Center, Defense Information Systems Agency, ATTN: Headquarters FOIA Requester Service Center, P.O. Box 549, Ft

Meade, MD 20755-0549. Signed, written requests should include the individual's full name, current address, telephone number, and the name and number of this system of records notice. In addition, the requester must provide 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 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: December 8, 2010, 75 FR 76426; June 16, 2014, 79 FR 34299

[FR Doc. 2021-17000 Filed: 8/9/2021 8:45 am; Publication Date: 8/10/2021]