BILLING CODE: 6001-FR

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2024-OS-0072]

Privacy Act of 1974; System of Records

AGENCY: Pentagon Force Protection Agency, 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, "Pentagon Facilities Access Control System," DPFPA 01. This system of records was originally established by the Pentagon Force Protection Agency (PFPA) to collect and maintain a listing of personnel who are authorized to access Pentagon Facilities and verify the identity of approved individuals with access to such facilities and offices. The system name is changing from "Pentagon Facilities Access Control System" to "Pentagon Facilities Access Control Records." This system of records notice (SORN) is being updated to expand the purpose for which the system of records was established and incorporate the DoD standard routines 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 [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 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: Mr. Dajonte Holsey, Pentagon Force Protection Agency, Department of Defense, 9000 Defense Pentagon, Washington DC 20301-9000, (703) 571-2939.

SUPPLEMENTARY INFORMATION:

I. Background

The Pentagon Facilities Access Control Records are maintained by the Pentagon Facilities and used to maintain a listing of personnel who are authorized to access Pentagon Facilities and verify the identity of approved individuals with access to such facilities and offices. The system name is changing from "Pentagon Facilities Access Control System" to "Pentagon Facilities Access Control Records." Subject to public comment, the DoD is updating this SORN to add 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 Authority for Maintenance of the System section to update citation(s) and add additional authorities; (2) 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; (3) to the Administrative, Technical, and Physical Safeguards to update the individual safeguards protecting the personal information; (4) to the Purpose of the System section to list the functions of the system with additional clarity; (5) to the Retention and Disposal section to reflect the approved disposition; (6) 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; (7) to the Contesting Records and Notification Procedures sections to update the appropriate citation for contesting records; and (8) to the System Manager and System Location sections to update the addresses and office names. 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 Defense for Privacy, Civil Liberties, and Transparency (OATSD(PCLT)) 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: June 24, 2024.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer,
Department of Defense.

SYSTEM NAME AND NUMBER: Pentagon Facilities Access Control Records, DPFPA 01.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION(S): 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):

A. Chief, Credentialing Branch, Security Services Division, Pentagon Force Protection Agency, 9000 Defense Pentagon, Washington, DC 20301-9000. Email: pfpa.pentagon.rsrcmgmt.list.ssd-pacb-ncic-requests-mbx@mail.mil, Phone: 703-697-9327.

B. Chief, Electronic Security Systems, Enterprise Physical Security Division, Pentagon Force Protection Agency, 9000 Defense Pentagon, Washington, DC 20301-9000.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. 113, Secretary of Defense; 10 U.S.C. 2674, Operation and Control of Pentagon Reservation and Defense Facilities in National Capital Region; 32 CFR 234, Conduct on the Pentagon Reservation, as amended; DoD Directive (DoDD) 5105.68, Pentagon Force Protection Agency (PFPA); DoDD 8521.01E, DoD Biometrics; DoD Instruction (DODI) 1000.25, DoD Personnel Identity Protection (PIP) Program; DoDI 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB); DoDI 5525.19, DoD Identity Matching Engine for Security and Analysis (IMESA) Access to Criminal Justice Information (CJI) and Terrorist Screening Databases (TSDB); DoD 5200.08-R, Physical Security Program; OSD Administrative Instruction 30, Force Protection on the Pentagon Reservation; Directive-Type Memorandum (DTM) 09-12, Interim Policy Guidance for DoD Physical Access Control, and E.O. 9397, as amended.

PURPOSE(S) OF THE SYSTEM: To collect and maintain records related to Pentagon Facility access and perimeter control, including visitor security and management. Additionally, to provision individual facility/installation access to an approved credential, and to verify the identity of an individual. The records will be vetted initially through the use of National Crime Information Center (NCIC), while continuous vetting occurs via the DoD Identity Matching Engine for Security and Analysis (IMESA) which may be accessed by other physical access control systems for further verification at other sites. The system may also be used for law enforcement purposes for verification and validation of recent and current police records.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Any Department of Defense military, civilian employee, or contractor sponsored by the Department of Defense, or other persons/visitors who have reason to enter Pentagon Facilities for official Department of Defense business. Other persons/visitors can include vendors, concessionaires, and domestic or foreign members of the press.

CATEGORIES OF RECORDS IN THE SYSTEM: Name, Social Security Number (SSN), DoD ID number, Federal Personal Identity Verification (PIV) Card Holder Unique Identifier (CHUID), foreign passport numbers, visa numbers, document numbers from Department of Homeland Security, race, sex, date of birth, place of birth, rank/grade, citizenship, photograph, digital certificates, biometric images and templates (e.g., fingerprint and iris), personal and work e-mail addresses and telephone numbers, employment information, name of DoD sponsoring office, background investigation type and completion date, date of issue and expiration of facility and installation access credentials, access level, previous facility pass issuances, authorizing official, and information that reflects time of entry and exit from a facility.

RECORD SOURCE CATEGORIES: Records and information stored in this system of records are obtained from the individual, U.S. Citizenship and Immigration Services Form I-9, the Identity Matching Engine for Security and Analysis (IMESA) system, or the Washington Headquarter Services Parking Database.

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, amended.

J. To such recipients and under such circumstances and procedures as are mandated by Federal statue 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. 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, SSN, DoD ID number, Federal PIV Card Holder Unique Identifier, or identification document that is compliant with the REAL ID Act (2005).

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Federal employees and contractors: Records are retained temporarily. Cut off upon terminating an employee's or contractor's term of employment. Destroy 6 years after cutoff. Official Visitors: Temporary. Cut off annually after final entry or after date of document, as appropriate. Destroy 5 years after cutoff.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: The Pentagon Facilities Access Control Records is physically secured using law enforcement personnel, contract security, physical access control and intrusion detection systems (ACS and IDS), and closed circuit TV (CCTV). Technical controls include user identification, passwords, firewalls, logical intrusion detection systems (IDS), encryption, DoD Public Key Infrastructure certificates and Common Access Cards (CAC). Administrative Controls include periodic security audits, regular monitoring of users' security practices, methods to ensure only authorized personnel have access to PII and encryption of backups containing sensitive data.

RECORD ACCESS PROCEDURES: Individuals seeking access to records about themselves in this system should address written inquiries to the Office of the Secretary of Defense/Joint Staff Freedom of Information Act Requester Service Center, Office of the Freedom of Information, 1155 Defense Pentagon, Washington, DC 20301-1155. Signed, written requests should contain the full name, SSN, DoD ID number or Federal PIV Personal Identifier (PI), current address and telephone number of the individual, and 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 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: May 9, 2011, 76 FR 26712.

[FR Doc. 2024-14203 Filed: 6/27/2024 8:45 am; Publication Date: 6/28/2024]