DEPARTMENT OF DEFENSE

Office of the Secretary of Defense

Narrative Statement on a Modified System of Records

Under the Privacy Act of 1974

1. System identifier and name: “Pentagon Facilities Access Control System,” DPFPA 01.

2. Nature of proposed modifications for the system: The Office of the Secretary of Defense is proposing to modify its system of records notice for Pentagon Facilities Access Control System, DPFPA 01. This system of records collects and maintains records related to Pentagon Facility access and perimeter control, including visitor security and management, to provision individual facility/installation access to an approved credential, and to verify individual’s identity. 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 person’s recent and current police records.

This SORN is being modified to be compliant with OMB Circular A108. In addition, it is updating OMB public information collection requirements, system location, categories of individuals, categories of records, authority, purpose, routine uses, retrievability, safeguards, retention and disposal, system manager(s) and address, notification procedure, record access procedures, and record source categories.

3. Authority for the maintenance (maintained, collected, used, or disseminated) of the system: 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 Manual 5200.08 v3, Physical Security Program: Access to DoD Installations; 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 (SSN), as amended.

4. Provide the agency’s evaluation on the probable or potential effects on the privacy of individuals: The PFPA ensured the safeguards for the system are compliant with DoD requirements and are appropriate to the sensitivity of the information stored within the system. Any specific routine uses have been reviewed to ensure the minimum amount of personally identifiable information and records retention between the DoD and other federal agencies, contractor companies and civilian organizations has been established. Visitor information is submitted through an auto-generated email containing a link to the Visitor Management System’s Pre-Registration portal, allowing the visitor to submit their personal information directly for vetting.

5. Routine use compatibility: The routine uses are consistent with the purpose for which the information was collected, and have been determined to be necessary and proper.

Routine use (a) is compatible with the purpose of the collection because it allows for sharing of information with personnel who maintain the Pentagon Facilities Access Control systems under contract with the PFPA.

Routine use (b), (c), (d), (e), (f) are compatible with the purpose of this collection because they would permit necessary and proper uses by enabling disclosures to the specific federal agencies identified in order to carry out their unique functions as stated in the routine uses.

Routine uses (g) and (h) are in response to the Office of Management and Budget (OMB) requirement in OMB M-17-12 to respond appropriately to a breach of personally identifiable information in this system of records or, as appropriate, to assist another Federal agency or entity in its response to a breach.

6. OMB public information collection requirements:

OMB collection required: Yes.

OMB Control Number (if approved): 0704-AAFV

Expiration Date (if approved) or Data submitted to OMB: The Federal Register Notice for this collection has published, the public comment period closed on 16 July

Provide titles of any information collection requests (e.g. forms and number, surveys, interviews scripts, etc.) contained in the system of records.

* DD FORM 2249, Pentagon Facilities Access Enrollment FORM
* Visitor Management System – Pre-Registration Web Portal
* PFPA FORM 79, Alarmed Space Access Request Form

If collecting on members of the public and no OMB approval is required, state the applicable exception(s): N/A.

**Information required by DPCLTD (not submitted to OMB).**

7. Name of IT system (state NONE if paper records only):

AMAG, DITPR 4282

DHHQ-ESS, DITPR 15612

LPRPE Mobile (license plate reader), DITPR 26046

PMP-2, DITPR 16185

SVSS, DITPR 18413

VCIN, DITPR 19195

MC-ESS, DITPR 15328

LSB, DITPR 16016

PSIM2, DITPR 38488

8. Is this system, in whole or in part, being maintained, collected, used, or disseminated by a contractor? Yes

**DEPARTMENT OF DEFENSE Billing Code:**

Office of the Secretary of Defense

**[Docket ID:**

Privacy Act of 1974; System of Records

**AGENCY:** Office of the Secretary of Defense, DoD.

**ACTION:** Notice to Modify a System of Records.

**SUMMARY:** The Office of the Secretary of Defense proposes to modify a system of records, titled “Pentagon Facilities Access Control System,” DPFPA 01. The Privilege Management Program was developed and deployed by PFPA as the identity management repository for both visitors and building tenants. This system of records facilitates background investigations for visitors and properly assigns access privileges to the building tenants for access to Pentagon Facilities protected by the Pentagon Force Protection Agency.

**DATES:** Comments will be accepted on or before [**INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].**  This proposed action will be effective on the date following the end of the comment period unless comments are received which result in a contrary determination.

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

\* Federal Rulemaking Portal: <http://www.regulations.gov>

Follow the instructions for submitting comments.

\* Mail: Department of Defense, Office of the Deputy Chief Management Officer, Directorate of Oversight and Compliance, 4800 Mark Center Drive, Mailbox #24, 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 <http://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

**FOR FURTHER INFORMATION, CONTACT:** Mrs. Luz D. Ortiz, Chief, Records, Privacy and Declassification Division (RPD2), 1155 Defense Pentagon, Washington, D.C. 20301-1155, or by phone at (571) 372-0478.

**SUPPLEMENTARY INFORMATION:** This system of records facilitates background investigations of visitors and building tenants and properly assigns privileges to the customer utilized within the Pentagon Reservation and National Capital Region (NCR). The system is also utilized for background investigations of individuals applying for access to the Pentagon in connection with Pentagon Tours.

The Privilege Management Program (PMP has allowed PFPA to ensure those requesting access have been properly vetted and possess the justifications necessary for access to locations needed to perform occupational duties. The system is necessary to facilitate background investigations and properly assign physical access within the Pentagon Reservation.

The following sections have been modified: system location, categories of individuals, categories of records, authority, purpose, routine uses, retrievability, safeguards, retention and disposal, system manager(s) and address, notification procedure, record access procedures, and record source categories.

The Office of the Secretary of Defense 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 http://defense.gov/privacy

The proposed systems report, as required by of the Privacy Act, as amended, were submitted on INSERT DATE, to the House Committee on Oversight and Government 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:

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

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

**SECURITY CLASSIFICATION:** Unclassified.

**SYSTEM LOCATIONS:**

Pentagon Force Protection Agency, 9000 Defense Pentagon, Washington, DC 20301-9000.

Pentagon Force Protection Agency, 4800 Mark Center Drive, Alexandria, VA 22350-3100.

Defense Health Headquarters, 7700 Arlington Boulevard, Falls Church, VA 22042-5101.

Raven Rock Mountain Complex, Liberty Township, PA 17320

**SYSTEM MANAGER(S):**

Chief, Credentialing Branch, Security Services Division, Pentagon Force Protection Agency, 9000 Defense Pentagon, Washington, DC 20301-9000. [pfpa.pentagon.rsrcmgmt.list.ssd-pacb-ncic-requests-mbx@mail.mil](mailto:pfpa.pentagon.rsrcmgmt.list.ssd-pacb-ncic-requests-mbx@mail.mil), Ph: 703-697-9327.

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. 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 (SSN), 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, to provision individual facility/installation access to an approved credential, and to verify individual’s identity. 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 person’s 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.

**CATEGORIES OF RECORDS IN THE SYSTEM:** Name, Social Security Number (SSN), DoD ID number, Federal Personal Identity Verification (PIV) Card Holder Unique Identifier (CHUID), document numbers from Department of Homeland Security, U.S. Citizenship and Immigration Services Form I-9 lists of verification documents, 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:** Individual, Department of Defense, Identity Matching Engine for Security and Analysis (IMESA), Washington Headquarter Services Parking Database

**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, 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:

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. To appropriate agencies, entities, and persons when (1) the DoD suspects or has confirmed that there has been a breach of the system of records; (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.
8. 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 STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:**

**POLICIES AND PRACTICES FOR STORAGE OF RECORDS:** Paper records in file folders and electronic storage media.

**POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:** Records are 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:**  Temporary. Cut off upon terminating an employee’s or contractor’s term of employment. Destroy 6 years after cutoff.

**ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:** The Pentagon Facilities Access Control System 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 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 published in 32 CFR part 310, or may be obtained from the System Manager.

**NOTIFICATION PROCEDURE:** Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to Credentialing Branch, Security Services Directorate, Pentagon Force Protection Agency, 9000 Defense Pentagon, Washington, DC 20301-9000.

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.

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**: May 9, 2011, 76 FR 26712