Billing Code: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2015-OS-0078]

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary of Defense, DoD.

ACTION: Notice to add a new System of Records.

SUMMARY: The Office of the Secretary of Defense proposes to add a new system of records, DPFPA 07, entitled "Counterintelligence Management Information System (CIMIS)" to conduct and exercise overall responsibility within PFPA for all matters pertaining to acts involving counterintelligence (CI) activities against PFPA employees, U.S. property, or interests. Also used as a management tool for statistical analysis, tracking, reporting, evaluating program effectiveness, and conducting research.

DATES: Comments will be accepted on or before [**INSERT 30-DAYS FROM DATE OF PUBLICATION IN THE FEDERAL REGISTER**]. This proposed action will be effective the day 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, Regulatory and Audit Matters Office, 9010 Defense Pentagon, Washington, DC 20301-9010.

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: Ms. Cindy Allard, Chief, OSD/JS Privacy Office, Freedom of Information Directorate, Washington Headquarters Service, 1155 Defense Pentagon, Washington, D.C. 20301-1155, or by phone at (571)372-0461.

SUPPLEMENTARY INFORMATION: The Office of the Secretary of Defense notices for systems of records subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended, have been published in the Federal Register and are available from the address in FOR FURTHER INFORMATION CONTACT or at http://dpcld.defense.gov/.

The proposed system report, as required by 5 U.S.C. 552a(r) of the Privacy Act of 1974, as amended, was submitted on July 30, 2015, to the House Committee on Oversight and Government Reform, the Senate Committee on Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to paragraph 4c of Appendix I to OMB Circular No. A-130, "Federal Agency Responsibilities for Maintaining Records About Individuals," dated February 8, 1996 (February 20, 1996, 61 FR 6427).

Dated: July 31, 2015.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

DPFPA 07

System name:

Counterintelligence Management Information System (CIMIS).

System location:

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

Categories of individuals covered by the system:

Any individual involved, or suspected of being involved, in intelligence collection on behalf of a foreign government or foreign terror organization which may harm PFPA employees, U.S. property or interests. Individuals involved in or suspected of being involved in National Security Crimes of assassination, sedition, subversion, treason, espionage, sabotage or terrorism. Individuals who provide information that is relevant to the case, such as victims or witnesses, and individuals who report such crimes or acts.

Categories of records in the system:
Data on suspect: Name; other names used (former and aliases); other identification (ID) numbers (e.g., DoD ID number, passport, VISA, resident alien); driver's license (state, number, and expiration date); date and place of birth; citizenship; legal status; gender; race/ethnicity; description (height, weight, hair color, etc.); name of current employer and address; college/university (major and/or degree); military records; home/office address; home/work/cell phone numbers; personal/work e-mail address; personal property information (e.g., vehicle, photographic equipment (make/model/serial number)); marital status; spouse location (city and state); and CIMIS incident number.

Data on individuals (victims, witnesses, complainant): Name; DoD ID number; work/home/cell phone numbers; and employer information (e.g. organization, address).

Additional data: Law Enforcement Reports; National Crime Information Center (NCIC); Intelligence Information Reports (IIR).

Individuals may voluntarily offer additional personal information in an effort to establish their identity. While not specifically requested, the information will be retained in the record if it is deemed beneficial to the inquiry.

Authority for maintenance of the system:
10 U.S.C. 2674, Operation and control of Pentagon Reservation and defense facilities in National Capital Region; 18 U.S.C. 794, Gathering or Delivering Defense Information to Aid Foreign Government; E.O. 12333, United States Intelligence Activities; E.O. 12968, Access to Classified Information; DoD Directive (DoDD) 5105.68, Pentagon Force Protection Agency (PFPA); DoDD 5200.27, Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense; DoDD 5240.01, DoD Intelligence Activities, as amended; DoDD 5240.02, Counterintelligence; DoDD 5240.06, DoD

Counterintelligence Awareness and Reporting (CIAR); DoD Instruction (DoDI) O-5240.21, Counterintelligence Inquiries; and Administrative Instruction 30, Force Protection on the Pentagon Reservation.

Purposes:

To conduct and exercise overall responsibility within PFPA for all matters pertaining to acts involving counterintelligence (CI) activities against PFPA employees, U.S. property, or interests. Also used as a management tool for statistical analysis, tracking, reporting, evaluating program effectiveness, and conducting research.

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:

To Federal counterintelligence and law enforcement agencies that administer programs or employ individuals involved in an incident or inquiry.

Law Enforcement Routine Use: If a system of records maintained by a DoD Component to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

Congressional Inquiries Disclosure Routine Use: Disclosure from a system of records maintained by a DoD Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

Disclosure to the Department of Justice for Litigation Routine Use: A record from a system of records maintained by

a DoD Component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

Disclosure of Information to the National Archives and Records Administration Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

Data Breach Remediation Purposes Routine Use: A record from a system of records maintained by a Component may be disclosed to appropriate agencies, entities, and persons when (1) The Component suspects or has confirmed that the security or confidentiality of the information in the system of records has been compromised; (2) the Component has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by

the Component or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Components efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

The DoD Blanket Routine Uses set forth at the beginning of the Office of the Secretary of Defense (OSD) compilation of systems of records notices may apply to this system. The complete list of DoD Blanket Routine Uses can be found online at: http://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx"

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:
Electronic storage media.

Retrievability:
Name, date of birth, and other identification (DoD ID number, passport, VISA or driver's license number).

Safeguards:

Electronically stored records are maintained in "fail-safe" system software with password-protected access. Access to these records is role-based and is limited to those individuals requiring access in performance of their official duties. Entry to the area is restricted by the use of cipher and combination locks, security guards, identification badges and closed circuit TV (CCTV). Data in transit and at rest is encrypted and computer servers are scanned to assess system vulnerabilities. Encryption of backups containing sensitive PII is in place. Firewalls are in place to control the incoming and outgoing data traffic based on an applied rule set. DoD Public Key Infrastructure Certificates are used to authenticate authorized users. Periodic security audits are maintained to document access to data. Regular monitoring of user's security practice is conducted and methods are used to ensure only authorized personnel have access to PII. All individuals granted access to this system of records receives annual Information Assurance and Privacy Act training.

Retention and disposal:

Files relating to Foreign Nationals: Close annually upon determination that the individual is no longer a threat to DoD,

the Pentagon, Pentagon Reservation or DoD Facilities within the Capitol Region (NCR). Destroy 25 year(s) after cut off.

Files relating to U.S. Citizens: Cut off after determination person(s) are no longer a CI threat to DoD, the Pentagon, Pentagon Reservation or DoD Facilities within the NCR. Destroy/delete 90 days after cut off.

System manager(s) and address:
Pentagon Force Protection Agency (PFPA), 9000 Defense Pentagon, Washington, DC 20301-9000.

Notification procedure:
An exemption rule has been published, and this Privacy Act system of records is exempt from the notification provisions described in 5 U.S.C. 552a(e)(4)(H).

Record access procedures:
An exemption rule has been published, and this Privacy Act system of records is exempt from the access provisions described in 5 U.S.C. 552a(d).

Contesting record procedures:

An exemption rule has been published, and this Privacy Act system of records is exempt from the amendment and appeal provisions described in 5 U.S.C. 552a(f).

Record source categories:
PFPA officers and investigators, state and local law enforcement, Federal departments and agencies, and intelligence agencies.

Exemptions claimed for the system:
This system of records is used by the Department of Defense for a law enforcement purpose (k)(2), and the records contained herein are used for criminal, civil, and administrative enforcement requirements. As such, allowing individuals full exercise of the Privacy Act would compromise the existence of any criminal, civil, or administrative enforcement activity. This system of records is exempt from the following provisions of 5 U.S.C. 552a section (c)(3), (d), (e)(1), (e)(4)(G) through (I), and (f) of the Act.

An exemption rule for this system has been promulgated in accordance with requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c), and (e) and published in 32 CFR part 311. For additional information contact the system manager.

[FR Doc. 2015-24792 Filed: 9/29/2015 08:45 am; Publication Date: 9/30/2015]