affecting personnel actions concerning members of the Armed Forces and or Federal employees; and to respond to other complaint investigations and congressional inquiries as appropriate.

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:

To the U.S. Secret Service in conjunction with the protection of persons under its jurisdiction.

To other Federal, State, local, or tribal agencies having jurisdiction over the substance of the allegations or a related investigative interest in criminal law enforcement investigations, including statutory violations, counter-intelligence, counter-espionage and counter-terrorist activities and other security matters.

To other Federal Inspector General offices, the President's Council on Integrity and Efficiency, and/or other Federal law enforcement agencies for the purpose of coordinating and conducting administrative inquiries and civil and criminal investigations, or when responding to such offices, Council, and agencies in connection with the investigation of potential violations of law, rule, and/or regulation.

To other Federal Inspector General offices, the President's Council on Integrity and Efficiency, and/or the Department of Justice for purposes of conducting external reviews to ensure that adequate internal safeguards and management procedures continue to exist within the Office of the Inspector General of the Department of Defense.

The DoD Blanket Routine Uses set forth at the beginning of the DISA's compilation of systems of records notices may apply to this system.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Electronic storage media and paper records.

RETRIEVABILITY:

By individual's name or case number.

SAFEGUARDS:

Computerized records maintained in a controlled area are accessible only to authorized personnel. Records are maintained in a controlled facility. Physical entry is restricted by the use of locks, guards, and is accessible only to authorized personnel. Physical and electronic access is restricted to designated individuals having a need therefore in the performance of official duties and who are properly screened and cleared for need-to-know. Electronic data system is password protected and will include data encryption of some fields. Access to computerized data is restricted by Common Access Card (CAC).

RETENTION AND DISPOSAL:

Electronic records are retained indefinitely for statistical purposes. Paper records for administrative investigations are archived 5 years after cases are closed. Paper records for criminal investigations are archived 20 years after cases are closed.

SYSTEM MANAGER(S) AND ADDRESS:

Chief, Investigations Division, DISA IG, 6910 Cooper Ave, Ft. Meade, MD 20755–7901.

NOTIFICATION PROCEDURE:

Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to Defense Information Systems Agency, ATTN: Headquarters FOIA Requester Service Center, P.O. Box 549, Ft Meade, MD 20755–0549.

Request should contain the individual's full name, SSN or DoD ID Number, current address for reply, and telephone number.

RECORD ACCESS PROCEDURES:

Individuals seeking access to information about themselves contained in this system should address written inquiries to Defense Information Systems Agency, ATTN: Headquarters FOIA Requester Service Center, P.O. Box 549, Ft Meade, MD 20755–0549.

Requests should contain the individual's full name, SSN or DoD ID Number, current address for reply, telephone number, and signature and provide a reasonable description of what they are seeking.

CONTESTING RECORD PROCEDURES:

Individuals seeking to contest contents and to appeal initial agency determinations should address written inquiries to Defense Information Systems Agency, ATTN: Headquarters FOIA Requester Service Center, P.O. Box 549, Ft Meade, MD 20755–0549.

RECORD SOURCE CATEGORIES:

Subjects and suspects of IG investigations. Interviews of witnesses, victims, and complainants. All types of records and information maintained by all levels of government, private industry, and non-profit organizations reviewed during the course of the investigation or furnished to the IG. Any other type of record deemed necessary to complete the IG investigation.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Parts of this system may be exempt pursuant to 5 U.S.C. 552a(j)(2) if the information is compiled and maintained by a component of the agency which performs as its principle function any activity pertaining to the enforcement of criminal laws.

Investigatory material compiled for law enforcement purposes may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source.

Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

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 316. For additional information contact the system manager.

[FR Doc. 2014–25806 Filed 10–29–14; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD–2014–OS–0125]

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 05, entitled ''Computer Aided Dispatch and Records Management System (CAD/RMS)'' to its inventory of record systems subject to

the Privacy Act of 1974, as amended. This system is used to record incident details related to PFPA investigations or inquiries into incidents under PFPA jurisdiction. Records may be used to develop threat analysis products, reports, and assessments on groups and individuals that have harmed, or have attempted harm; made direct or indirect threats; have a specific interest in high ranking Office of the Secretary of Defense (OSD) personnel, the DoD workforce, or the Pentagon Facilities; or have engaged in organized criminal activity that would impact the Pentagon Facilities. These records are also used to document incident updates (if additional evidence is gathered following initial contact).

DATES: Comments will be accepted on or before December 1, 2014. 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:* Federal Docket Management System Office, 4800 Mark Center Drive, East Tower, 2nd Floor, Suite 02G09, Alexandria, VA 22350–3100.

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, DC 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://dpclo.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, 2014, 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: October 27, 2014.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

DPFPA 05

SYSTEM NAME:

Computer Aided Dispatch and Records Management System (CAD/RMS).

SYSTEM LOCATION:

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

Pentagon Force Protection Agency (PFPA), 4800 Mark Center Drive, Alexandria, VA 22350.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who have been the subject of an investigation or police inquiry into incidents occurring at the Pentagon and other facilities under the jurisdiction of PFPA.

CATEGORIES OF RECORDS IN THE SYSTEM:

Incident report contains any or all of the following: name; other names used; Social Security Number (SSN); citizenship; legal status; gender; race/ethnicity; employment (e.g., authorized access to the building or room), and education information (e.g., student ID as form of identification); military records; driver's license; other identification numbers (e.g., DoD ID number, passport); date and place of birth; home and office address; home, work, and cell phone numbers; personal email address; photos taken at the scene; personal property information (e.g., vehicle, photographic equipment); biometric information (e.g., fingerprints); handwriting samples (e.g., scans of letters written by the subject mailed to the facility); child information (e.g., in cases where a child needs to be picked up if a parent is arrested), or contact information (e.g. spouse or an adult to provide transportation/assistance, if necessary); medical information (e.g., collected during medical response calls to assist individual); emergency contact, and incident number.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

10 U.S.C. 2674, Operation and Control of Pentagon Reservation and Defense Facilities in National Capital Region; DoD Directive 5105.68, Pentagon Force Protection Agency (PFPA); Administrative Instruction (AI) 30, Force Protection on the Pentagon Reservation; and E.O. 9397 (SSN), as amended.

PURPOSES:

To record incident details related to PFPA investigations or inquiries into incidents under PFPA jurisdiction. Records may be used to develop threat analysis products, reports, and assessments on groups and individuals that have harmed, or have attempted harm; made direct or indirect threats; have a specific interest in high ranking Office of the Secretary of Defense (OSD) personnel, the DoD workforce, or the Pentagon Facilities; or have engaged in organized criminal activity that would impact the Pentagon Facilities. These records are also used to document incident updates (if additional evidence is gathered following initial contact).

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:

DoD Routine Use 01, Law Enforcement. 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.

To insurance agencies representing an individual who has been the subject of an investigation or police inquiry into incidents occurring at the Pentagon and other facilities under the jurisdiction of PFPA.

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.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Paper records in file folders and electronic storage media.

RETRIEVABILITY:

Name, SSN, date of birth, other names used, driver license, or incident number.

SAFEGUARDS:

Records are maintained in areas accessible only to PFPA law enforcement personnel who use the records to perform their duties. All records are maintained on DoD installations with security force personnel performing installation access control and random patrols. Common Access Cards (which contain the user's DoD Public Key Infrastructure Certificates) and personal identification numbers are used to authenticate authorized desktop and laptop computer users. Data in transit and at rest is encrypted and computer servers are scanned to assess system vulnerabilities. Specific firewalls are in place to control the incoming and outgoing data traffic by analyzing the data and determining whether they should be allowed through or not, based on applied rule set. User access is restricted to validated users and activity is regularly monitored. Systems security updates are accomplished on a regular basis. Records are secured in locked or guarded buildings monitored by Closed Circuit TV cameras and intrusion detection systems, locked offices (to include cipher locks), or locked cabinets during non-duty hours, with access restricted during duty hours.

RETENTION AND DISPOSAL:

Non-criminal records are destroyed one year after case is closed.

Criminal records are cut off when a case is closed. Files are destroyed 15 years after the cut-off.

SYSTEM MANAGER(S) AND ADDRESS:

Deputy Director Integrated Emergency Operations Center, 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(d).

RECORD ACCESS PROCEDURES:

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(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:

Individuals involved in, or witness to, the incident or inquiry, PFPA officers and investigators, state and local law enforcement, and Federal departments and agencies.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

This system of records is used by the Department of Defense for a law enforcement purpose (j)(2) and (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) and (4), (d), (e)(1) through (e)(3), (e)(4)(G) through (e)(4)(I), (e)(5), (e)(8); (f) and (g) 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. 2014–25834 Filed 10–29–14; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD–2014–OS–0092]

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary of Defense, DoD.

ACTION: Notice to alter a System of Records.

SUMMARY: The Office of the Secretary of Defense proposes to alter a system of records, DWHS E05, entitled ''Mandatory Declassification Review Files'', in its inventory of record systems subject to the Privacy Act of 1974, as amended. This system is used to process requests and/or appeals from individuals for the mandatory review of classified documents for the purposes of releasing declassified material to the public; and to provide a research resource of historical data on release of records to ensure consistency in subsequent actions. Data developed from this system is used for the annual report required by the applicable Executive Order(s) governing classified National Security Information. This data also serves management needs, by providing information about the number of requests; the type or category of records required; and the average processing time.

DATES: Comments will be accepted on or before December 1, 2014. This proposed action will be effective 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:* Federal Docket Management System Office, 4800 Mark Center Drive, East Tower, 2nd Floor, Suite 02G09, Alexandria, VA 22350–3100.

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, DC 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 the Defense Privacy and Civil Liberties Office Web site at *http://dpclo.defense .gov/.*

The proposed system report, as required by U.S.C. 552a(r) of the Privacy Act of 1974, as amended, was submitted on June 9, 2014, 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