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: Computer Aided Dispatch and Records Management System (CAD/RMS), DPFPA 05.

2. Nature of proposed modifications for the system: The Office of the Secretary of Defense proposes to modify a system of records that allows PFPA to more efficiently dispatch its police officers to incidents and acts as a repository for data gathered on scene that can later be used for reporting purposes or criminal investigations. The technology simplifies information exchange across emergency management, law enforcement and investigative personnel. The system will record incident details related to PFPA investigations or inquiries into incidents under PFPA jurisdiction. These records are also used to document incident updates (if additional evidence is gathered following initial contact).

This modification updates the categories of records, authority, routine uses, safeguards, and record source categories.

3. Authority for the maintenance of the system: 10 U.S.C. 2674, Operation and control of Pentagon Reservation and defense facilities in the National Capital Region; 28 CFR 23, Criminal Intelligence Systems Operating Policies-Operating principles; DoD Directive (DoDD) 5105.68, Pentagon Force Protection Agency (PFPA); DoD Instruction (DoDI) 0-2000.22, Designation and Physical Protection of DoD High Risk Personnel; DoDI 5525.18, Law Enforcement Criminal Intelligence (CRIMINT) in DoD; Administrative Instruction 30, Force Protection on the Pentagon Reservation; 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.

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

6. OMB public information collection requirements:
OMB collection required: Yes
OMB Control Number (if approved): 0704-0522
Expiration Date (if approved): 11/30/17

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

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): Computer Aided Dispatch and Records Management System (CAD/RMS), DITPR 16861.

8. Is this system, in whole or in part, being maintained, collected, used, or disseminated by a contractor? Yes, contractors perform IT administrator functions for the system.

Billing Code:
DEPARTMENT OF DEFENSE
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 of a Modified System of Records.

SUMMARY: The Office of the Secretary of Defense proposes to modify a system of records, Computer Aided Dispatch and Records Management System (CAD/RMS), DPFPA 05. The CAD/RMS is a software technology solution allowing PFPA to more efficiently dispatch its police officers to incidents and acts as a repository for data gathered on scene that can later be used for reporting purposes or criminal investigations. The technology simplifies information exchange across emergency management, law enforcement and investigative personnel.

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: The Computer Aided Dispatch and Records Management System (CAD/RMS), software technology solution allows PFPA to more efficiently dispatch its police officers to incidents and acts as a repository for data gathered on scene that can later be used for reporting purposes or criminal investigations. The technology simplifies information exchange across emergency management, law enforcement and investigative personnel.

Data is input directly into the database by PFPA's Pentagon Police and its emergency management personnel. The application provides open text fields and drop-down options for inputting non-standard and standard data, respectively. Only PFPA personnel with an active Police Dispatch and Investigatory Records System account and DoD-issued Common Access Card (CAC) can access the data and update reports. All modifications to reports are tagged with a date/time stamp and the PFPA personnel's identity.

As a result of reviewing this system of records notice, the PFPA proposes to modify the following sections: System Name, Authority for Maintenance of the System, Purpose, Safeguards, Categories of Records, Routine Uses, and added History.

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 reports, 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: Police Dispatch and Investigatory Records, DPFPA 05.

SECURITY CLASSIFICATION: Unclassified.

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.

SYSTEM MANAGER(S) AND ADDRESS: Deputy Director Integrated Emergency Operations Center, Pentagon Force Protection Agency (PFPA), 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 the National Capital Region; 28 CFR 23, Criminal Intelligence Systems Operating Policies-Operating principles; 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; DoD Instruction (DoDI) 0-2000.22, Designation and Physical Protection of DoD High Risk Personnel; DoDI 5525.18, Law Enforcement Criminal Intelligence (CRIMINT) in DoD; Administrative Instruction 30, Force Protection on the Pentagon Reservation; and E.O. 9397 (SSN), as amended.

PURPOSE(S) OF THE SYSTEM: To record incident details related to PFPA criminal and threat investigations or law enforcement calls for within PFPA's jurisdiction including medical assists. 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).

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: Name; other names used; Social Security Number (SSN); citizenship; legal status; gender; race/ethnicity; employment (e.g., authorized access to the building or room), marital status and education information (e.g., student ID as form of identification); military and law enforcement 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 e-mail address; photos taken at the scene; personal property information (e.g., vehicle make, model, body style and license plate; photographic equipment); biometric information (e.g., hair color, eye color, 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.

RECORD SOURCE CATEGORIES: Individuals involved in, or witness to, the incident or inquiry, PFPA officers and investigators, state and local law enforcement (e.g. National Crime Information Center/Virginia Crime Information Network) and Federal departments and agencies, (e.g. Naval Criminal Investigative Service, Federal Bureau of Investigation).

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USERS:

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:

a. 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.

b. To an appeal, grievance, or formal complaints examiner; equal employment opportunity investigator; arbitrator; exclusive representative; or other officials engaged in investigating, or settling a grievance, complaint or appeal filed by an employee.

c. To various bureaus and divisions of the Department of Justice that have primary jurisdiction over subject matter and location which PFPA shares.

d. To contractors 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.

e. 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.

f. 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.

g. 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.

h. 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.

i. 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.

j. 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.

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

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: 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.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL 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. All records are physically secured using security guards, cipher/combination locks, identification badges, key cards, safes and closed circuit TV (CCTV). Technical controls include user identification, passwords, firewalls, intrusion detection system (IDS), DoD Public Key Infrastructure certificates, Virtual Private Network (VPN), encryption and Common Access Card (CAC). Administrative controls

include periodic security audits, regular monitoring of users' security practices methods to ensure only authorized personnel have access to Personally Identifiable Information (PII) and encryption of back-up and recovery Standard Operating Procedures.

RECORD ACCESS 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).

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).

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).

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.

HISTORY: October 30, 2014, 79 FR 64582.