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, passport, etc.); 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, photographic equipment); biometric information (e.g., fingerprints); handwriting samples (e.g., scans of letters written by the subject mailed to the facility); child information or spouse information (e.g., child requiring assistance if parent is arrested or spouse/child able to retrieve individual if necessary), present location); 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 (DoDD) 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:

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.