PRIVACY IMPACT ASSESSMENT (PIA)

For the

Computer Aided Dispatch / Records Management System
Pentagon Force Protection Agency

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐	**New DoD Information System**	☒	**New Electronic Collection**
☒	**Existing DoD Information System**	☐	**Existing Electronic Collection**
☐	**Significantly Modified DoD Information System**		

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒	**Yes, DITPR**	Enter DITPR System Identification Number	16861
☐	**Yes, SIPRNET**	Enter SIPRNET Identification Number	
☐	**No**		

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☐ **Yes** ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier DPFPA-05

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date. Submission pending

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number | Submission pending

Enter Expiration Date |

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

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

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

To record incident details related to 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. In addition, used to record updates if additional evidence is gathered following initial contact. The information is collected from 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. The incident report contains any or all of the following categories of information: Name; other names used; Social Security Number (SSN); citizenship; legal status; gender; race/ethnicity; medical, employment, and education information; 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., existence, present location); medical information (e.g., medical response calls); emergency contact, and incident number.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The Privacy risks may include threats, including, but not limited to: malware, sniffing, spoofing, insider threat, as well as various natural disasters and failures which impact either the protected infrastructure or the services upon which the infrastructure depends. All of these imperil, to one extent or another, information availability and integrity and are minimalized by a number of safeguards such as: records are maintained in a controlled facility; physical entry is restricted by the use of locks and guards and is accessible only to authorized personnel; access is records is limited to person(s) responsible for servicing the record in performance of their official duties and who are properly screened and cleared for need-to-know; access to computerized data is restricted by CAC and username/ passwords, which are changed periodically; and data is natively encrypted at the Operating System level. In addition, periodic security audits are performed.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. Officers and Supervisors, Records Clerks, Investigators

☒ **Other DoD Components.**

Specify. Law Enforcement Defense Data Exchange

☒ **Other Federal Agencies.**

Specify. Federal agencies that employ individuals involved in an incident or inquiry. Agencies charged with the responsibilities of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto for the purpose of supporting law enforcement efforts

☒ **State and Local Agencies.**

Specify. State or local agencies that employ individuals involved in an incident or inquiry. Agencies charged with the responsibilities of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto for the purpose of supporting law enforcement efforts

☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

☒ **Other** (e.g., commercial providers, colleges).

Specify. 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.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Disclosure is voluntary, however, failure to provide requested information may result in the individual being subject to arrest if a criminal act has occurred. Once in custody, disclosure is voluntary and non-disclosure notated in the arrest record.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

The Pentagon Force Protection Agency requires collection of information from members of the public during the course of investigating criminal or suspicious activity incidents and medical responses in order to positively identify respondents and collect information pertinent to the medical assistance and investigation and/or criminal prosecution of persons involved.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ **Privacy Act Statement** ☐ **Privacy Advisory**

☐ **Other** ☐ **None**

Describe each applicable format.

Authority: 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.

Principle Purpose: To record incident details related to PFPA investigations or inquiries into incidents under PFPA jurisdiction.

Routine Uses: 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. DoD Blanket Routine Use (1) Law Enforcement specifically applies to this system. Other DoD Blanket Routine Uses found at http://dpclo.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx may apply to these records. Any release under a blanket routine use will be compatible with the purpose of the collection.

Disclosure: Voluntary, however, failure to provide identifying information may result in the individual being subject to arrest if a criminal act has occurred. Once in custody, disclosure is voluntary and non-disclosure notated in the arrest record.. The use of the SSN is strictly to ensure accurate identification of the individual.