PRIVACY IMPACT ASSESSMENT (PIA)

For the

Air Force Safety Automated System (AFSAS)
United States Air Force (USAF)

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: 170
- ☐ **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 007-57-01-03-01-8064-00

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 F032 AF ILE

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.

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

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.

Occupational Safety and Health Administration's (OSHA) reporting requirements in accordance with E.O. 12196 and 29 CFR 1960; Executive Order (EO) 9397 (use of Social Security Numbers); Department of Defense Instruction 6055.7, Accident Investigation, Reporting, and Record Keeping and its references; and, 10 U.S.C. 8013 (Secretary of the Air Force, powers and duties).
Agency Authority includes: AFI 91-204 Safety Investigation and Reports and DODI 65055.7 Accident Investigation, Reporting, and Record Keeping.

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.

AFSAS was developed to be the single source for all USAF safety disciplines to report mishaps and query the resulting data. The goal is to produce valid and reliable data, to implement the operational risk management (ORM) process and prevent mishaps. Present life cycle phase is development. AF/SE is the system sponsor. The system resides on the NIPERNET within a .mil hosted domain. The system is located at HQ AFSC, Kirkland AFB NM in building 24499. The system has both an on line transaction processing and data warehouse component including backup capability at 377 ABW Kirtland AFB NM.

Information is collected of those involved in mishaps and witnesses (could be members of the general public) to include names, social security numbers, age, and medical information (Injury Severity, Injured Body Part, and Injury Type).

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

AFSAS can only be accessed via Common Access Card (CAC) technology. The card contains advanced technology, which identifies, controls, and accounts for users entering the AFSAS application. AFSAS user accounts are approved at MAJCOM level, new users are entered into the User Administration database as authorized users. When the user first enters the AFSAS application, his/her CAC is authenticated against the authorized user database.

To ensure AFSAS is only used for lawful purposes, the activities of individuals may be electronically monitored at any time. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action.

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. Shared with Air Force clinics and safety offices

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify.

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

Specify.

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.

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

All DoD personnel must provide their information. Other personnel, including contractors, consent before providing the information. After the information is collected, it cannot be used to generate a System of Records report and may only be used for mishap prevention analysis. For example, a person's name and injury type is never generated in a report, only the aggregate numbers and primary causes are generated for analysis purposes.

During a mishap investigation a privacy case flag is set in AFSAS by the investigator when interviewing an injured person involved in a mishap. This prevents privacy data from being viewed by persons not involved in the investigation and prevents it reported on the OSHA 300 Log report to Department of Labor. However, once the preliminary message has been released in the AFSAS system, and during the course of a mishap investigation, the investigation board can see privacy information. Once the investigation is closed privacy information cannot be seen. The one exception is that HQ AFSC personnel (approximately four individuals) with the quality control role granted can see privacy information at any time.

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.

AFSAS can only be accessed via Common Access Card (CAC) technology. The card contains advanced technology, which identifies, controls, and accounts for users entering the AFSAS application. AFSAS user accounts are approved at MAJCOM level, new users are entered into the User Administration database as authorized users. When the user first enters the AFSAS application, his/her CAC is authenticated against the authorized user database.