PRIVACY IMPACT ASSESSMENT (PIA)

For the

Security Forces Management Information System (SFMIS)
U. S. Air Force

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	67
☐	**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 007-57-01-27-01-1687-00

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 F031 AF SF B

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.

10 United States Code (USC) 8013, Secretary of the Air Force; DoD Directive 7730.47, Defense Incident Based Reporting System (DIBRS); Air Force Instruction 31-203, Security Forces Management Information System; 18 USC 922 note, Brady Handgun Violence Prevention Act; 28 USC 534 note, Uniform Federal Crime Reporting Act; 42 USC 10601 et seq., Victims Rights and Restitution Act of 1990; Executive Order (EO) 9397 (Social Security number), 44 USC 3101, and 18 USC 922(d) (9) Lautenberg Amendment.

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.

Serves as a repository of criminal and specified other non-criminal incidents used to satisfy statutory and regulatory reporting requirements, specifically crime statistics required by the Department of Justice (DoJ) under the Uniform Federal Crime Reporting Act; to provide personal information required by the DoJ under the Brady Handgun Violence Prevention Act; and statistical information required by DoD under the Victim's Rights and Restitution Act. The system is used to enhance Air Force's capability to analyze trends and to respond to executive, legislative, and oversight requests for statistical crime data relating to criminal and other high-interest incidents.

The system is the primary host of all United States Air Force (USAF) vehicle and private weapon registration, visitor pass and restricted area authorization tracking. Other operations include capabilities to track combat arms training and qualifications, that include the last qualified date, score, and next due date by individual weapon and course of fire. Weapon maintenance, inventory control, and tracking, modification, inspection, and weapon firing are recorded in the combat arms function, and munitions expenditure.

Combat arms include the maintenance of range facilities. Security Forces Management Information System (SFMIS) tracks the scheduling of range and equipment usage, inspection and maintenance. Certification records for other agencies to utilize the range are also maintained in this system. Most recently it provides a direct interface with the National Crime Information Center (NCIC) and Integrated Automated Fingerprint Identification System (IAFIS) as hosted by the Federal Bureau of Investigations (FBI) via the Criminal Justice Information System (CJIS).

The system hosts Federal Application User Fee (FAUF) transactions for civilians applying for federal employment. FAUF is a format required for any branches of the U.S. military in connection with individual's enlisting, Officer Candidate School, federal agencies in connection with employment, security updates, or contract personnel. This module includes an Office of Personnel Management (OPM) FAUF transaction used to transmit FAUF transactions to the Air Force Office of Personnel & Management. Additionally, the system tracks accident reporting, providing user input and tracking for traffic accidents.

The system generates reports for use by the Air Force Security Forces at all levels of command, provides security forces commanders the ability to view criminal statistics and apply whatever actions are necessary for enforcement."

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

Records are accessed by person(s) responsible for servicing the record system in performance of their official duties, and by authorized personnel who are properly screened and cleared for need-to-know. It is up to each administrator to ensure this requirement is complied with, before access is granted. There is a potential risk that administrator's could fail to ensure these requirements are met for each user they grant access.

Records are stored in computer storage devices protected by computer system software.

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. Air Force Staff Judge Advocate, AF Office of Personnel Management, Unit Training Monitors, Air Force Office of Special Investigations, Automated Military Justice Analysis and Management System, Deployment Readiness Service

☒ **Other DoD Components.**

Specify. U. S. Army Provost Marshall's Office, Defense Manpower Data Center,

☒ **Other Federal Agencies.**

Specify. Federal Bureau of Investigations, National Criminal Justice Information Center

☐ **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.

The Air Force rules for accessing records, contesting contents and, appealing initial agency determinations are published in Air Force Instruction 33-332, Privacy Act Program; 32 Code of Federal Regulations (CFR) part 806b; or may be obtained from the system manager.

Data collection processes involve the use of authorized forms that stipulate the authority and need for the data. When dealing with recorded action involving the violation of federal or state law, an offender may not withhold information that is used to identify the person, validate identity, or locate the offender.

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.

In cases where voluntary disclosure is necessary, the uses of authorized DoD or USAF Forms or posted signs in Customer Service areas are used. As mentioned previously, the forms or postings will stipulate the authority and need. A denial of service may occur depending on the nature of the service request, if not provided.

In one case, the SFMIS system collects data directly from an individual requesting registration services. During the process, the screen capturing personal data includes a WARNING/CAVEATE that explains the authority, purpose, and results if the information is not disclosed.

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

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.

If used, DoD and USAF forms have the Privacy Act posted in the header. These forms are provided to the recipient in person and collected in the same manner. In some cases in Registration Services, a sign will be posted with electronic disclosure; when used in Kiosk or Web registration services, a notice titled Caveat/Privacy Act is offered.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.