PRIVACY IMPACT ASSESSMENT (PIA)

For the

Automated Case Tracking System (ACTS 5.0)
United States 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	9508
☐	**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 F90 AF IG B; (ACTS 5.0); Dec 25, 2008 69 FR 44515

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. 9 July 08

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.

The authority to collect Privacy Act (PA) information is derived from
10 United States Code (USC) 8013, Secretary of the Air Force: powers and duties; delegation by
10 U.S.C. 8020, Inspector General, and E.O. 9397 (SSN);

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.

ACTS is a records repository and a cradle-to-grave case management tool for IG personnel. Information is used to ensure just, thorough and timely resolution; to respond to complaints, allegations or queries; and to improve morale, welfare, and efficiency of organizations, units, and personnel by providing an outlet for redress.
Records may indicate where commander involvement is needed to correct systemic, programmatic, or procedural weakness and ensures resources are used effectively and efficiently

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

The perceived threats are primarily computer hackers, disgruntled employees, and acts of nature (e.g. fire, flood, etc).

Records are accessed by custodian of the system of records and by person(s) responsible for servicing the record system in performance of their official duties who are properly screened and cleared for need-to-know. Records are stored in a locked room protected by cipher lock. Records are controlled by personnel screening and protected by security alarm system. Information maintained on electronic media is protected by computer system software and password. CAC; .mil domain.

Confidentiality. This ensures that data is not made available or disclosed to unauthorized individuals, entities, or processes.

Integrity. This ensures that data is not been altered or destroyed in an unauthorized manner.

Training. Security training is provided on a continuous basis to keep users alert to the security requirements. Visual effects are used as constant reminders to ensure users always remain aware of their responsibilities.

Physical Security. This consists of placing servers that contain privileged information in a secure and protected location, and to limit access to this location to individuals who have a need to access the servers.

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 Board of Military Corrections and Judge Advocate staff

☐ **Other DoD Components.**

Specify.

☒ **Other Federal Agencies.**

Specify. FBI and OPM personnel

☒ **State and Local Agencies.**

Specify. State Courts through subpoena, access and release will be based on decisions of the courts

☐ **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.

Individuals do not have the option to object to the Privacy Act information being entered into ACTS since the information is germane to a specific investigation and the PII is essential to identifying indivdiuals.

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 data in ACTS is required for Inspector General to carry out their statutory duties.

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.

Privacy Advisory:

During the course of this interview, I will ask you to furnish information about yourself. The Privacy Act of 1974 requires that I inform you of the authority for this requirement. The statement, which I am now handing you, serves this purpose (hand statement to witness). Please read the statement at this time

Privacy Act Statement:

Policy: The Privacy Act statement is required to be read and acknowledged by each witness at the beginning of the interview process.

Authority: Title 10, United States Code, Sections 8013 and 8020, and Executive Order 9397 (SSN).

Principal Purpose: Information is collected during an inquiry or investigation to aid in determining the facts and circumstances surrounding the allegations. The information is assembled in report format and presented to the Appointing Authority as a basis for DoD or Air Force decision-making.
The information may be used as evidence in judicial or administrative proceedings or for other official purposes within the DoD. Disclosure of Social Security number, if requested, is used to further identify the individual providing the testimony.

Routine Uses: Routine uses include:

Forwarded to federal, state, or military and local law enforcement agencies for law enforcement purposes
Used as a basis for summaries, briefings, or responses to members of Congress or other agencies in the Executive Branch of the Federal Government
Provided to Congress or other federal and state agencies when determined to be necessary by The Inspector General, USAF
Any of the blanket routine uses published by the Air Force

Mandatory or Voluntary Disclosure:
FOR MILITARY PERSONNEL: Disclosing your Social Security number is voluntary. Disclosing other personal information relating to your position responsibilities is mandatory and failure to do so may subject you to disciplinary action.

FOR DEPARTMENT OF THE AIR FORCE CIVILIANS Disclosing your Social Security number is voluntary. However, failure to disclose other personal information in relation to your position responsibilities may subject you to adverse personnel action.

FOR ALL OTHER PERSONNEL: Disclosing your Social Security number and other personal information are voluntary. No adverse action can be taken against you for refusing to provide information about you.

Receipt Acknowledged , Date Signed

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.