PRIVACY IMPACT ASSESSMENT (PIA)

For the

F-22 Integrated Digital Environment (F-22 IDE)
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: 2006
- ☐ **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 - 1302 - 00 - 404 - 142

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 F036 AF A

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 U.S.C. 8013, Secretary of the Air Force 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.

The F-22 Integrated Digital Environment (IDE) is a decision support tool that serves as a single access point for unit information within a web-enabled environment. A component of the IDE is an application that automates the in and out-processing of unit personnel. Information collected during in-processing is used to initiate establishment of personnel records within the unit.

The following identifiable information is collected on unit members

- Name
- Citizenship
- Mailing/Home Address
- Emergency Contact
- Birth Date
- Home Telephone Number
- Employment Information
- Education Information
- Social Security Number (SSN)
- Place of Birth
- Military Records

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

Risks:
A number of employees within the unit Human Resources Department have access to the data collected. The risk associated with this access is based on the potential turnover of personnel and the integrity of the personnel handling the data. All personnel that have access to the data are required to have, at a minimum, a favorable National Agency Check on file.
As with any online IT system, the IDE is subject to intrusion and exploitation attempts. This risk is mitigated based on a robust, multi-layer security plan for the IDE that includes a firewall, inbound domain restrictions, 128-bit SSL data encryption and PKI/Windows user identification/authentication.

Safeguard Measures:
Administrative: Policies and procedures exist within the 478 AESG that define what information will be made available to individuals within the unit. Personnel requesting information must demonstrate a valid need to know and must be requesting the information in the performance of official duties within the unit.
Physical: Web servers containing the information are secured within the Acquisition Management Complex (AMC), Area B, Building 20553 at WPAFB OH. Access to Acquisition Management Complex buildings requires the use of a magnetic swipe card and personal 4-digit Personal Identification Number (PIN). Each building and separate access controlled areas within the buildings have swipe card readers that are programmed for different zones. Only individuals who support the acquisition programs located in Building 20553 are issued a swipe card with the appropriate zones for access and a PIN number. IDE servers are located within the 478 AESG restricted areas, in a secured network computer room, Room 081 of Building 20553. Only system administrators, security personnel and the facility manager have swipe card access to this computer room.
Technical: The IDE web server is protected by the Wright-Patterson AFB firewall and is restricted for inbound traffic on the *.mil network only. Access to the F-22 IDE is further controlled through use of Public Key Infrastructure (PKI) security and Windows Authentication. The combination of these security techniques ensures only authorized users log into the system and provides positive identification and authentication of each user within the IDE. Authorized users within the IDE are limited to only that data they are authorized access to, based on their defined IDE user profile. After the user credentials have been verified, a session cookie is established for that user and serves to maintain the user profile and permissions during the session. This cookie is non-persistent and is terminated at the end of each IDE session.

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. Only those persons within the 312th AESW and 478th AESG who have a verifiable need for access to the records in performance of their official duties have access to the record system. The information collected is primarily used and maintained by the Human Resources Department. Additionally, during in-processing, certain agencies within the unit will have access to the data as necessary to facilitate in-processing the member. The information is not released to anyone outside the unit.

☐ **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.

All personal data collected is voluntarily given by the subject individual. The entry page to the site includes a Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), allowing the individual to make an informed decision about providing the data. The statement advises the individual that the information provided is voluntary and provides the consequences of choosing not to participate with the information collection. Individuals may raise an objection with the Air Force Privacy Act office during the public comment period of the Privacy Act system of records notice (if applicable) or during the data collection.
The subject individual initiates the collection and maintenance of his/her information for the purpose of establishing a personnel record within the unit. Release of this information is done with the individual's full cooperation and consent.

(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.

A Privacy Act system of records notice exists within the Federal Register. The entry page to the site includes a Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), allowing the individual to make an informed decision about providing the data or participating in the program. Individuals may raise an objection with the Air Force Privacy Act Office during the comment period, during data collection, or at any time after the program is launched. If no objections are received, consent is presumed.
AFI 33-332, "Privacy Act Program", http://www.e-publishing.af.mil/pubfiles/af/33/afi33-332/afi33-332.pdf , governs Privacy Act data collections in the Air Force. AFI 33-129, "Web Management and Internet Use", http://www.e-publishing.af.mil/pubfiles/af/33/afi33-129/afi33-129.pdf discusses data collection and privacy policies. Air Force civilian employees, military members, and contractors are required to be aware of Privacy Act issues (e.g. via Privacy Act training offered by your MAJCOM/DRU/FOA/base, http://www.foia.af.mil/Privacy/Tng1.shtml, etc.) to fulfill their duties in handling third party personal data and in learning their Privacy Act rights.

(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.

The users edit/submit their information via the web application interface provided. Upon authentication of the user to the web site, they are presented with a Privacy Act Statement, informing them of the need to collect certain personally identifiable information, the authority to do so, their rights under law and routine uses of the data collected. The Privacy Act Statement is available to the user from within the application at all times.

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.