PRIVACY IMPACT ASSESSMENT (PIA)

For the

Enterprise Business System
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	1117
☐	**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 007-57-01-16-01-0478-00

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 F036 AF PC C

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.

Title 10, United States Code, Section 8013; Executive Order (EO) 9397 (Social Security Number - 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.

Collaborative Work Environment (CWE) - The CWE supports the Air Force Research Laboratory (AFRL) goal of providing an environment that allows better sharing of information and communication among AFRL personnel and customers, providing faster development and transition of technology. The CWE provides a central location for document management, records management, and collaboration. As a result, the CWE provides AFRL with an ability to collaborate effectively across the entire AFRL enterprise.
Awards and Decorations - Within the CWE, the Awards and Decorations process was developed based on internal AFRL request to automate the document management and approval process for awards and decoration given to enlisted and officer personnel within the Labs. The use of the automated Awards and Decorations process has substantially reduced lost documentation and has allowed AFRL management better insight into the status of each award/decoration. Personal information collected: Name, Other Names Used, SSN, Home & Office Addresses, Home & Office Phone numbers, Personal & Business E-mail, Military Records, Emergency Contact, Professional Certificates, Security Clearance, Electronic Data Interchange Personal Identifier (EDIPI).

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

Privacy risks regarding PII collected for storage within the CWE and the Awards and Decorations Workflow stem from the potential for unauthorized access to the Enterprise Business System (EBS) Family of Systems or the unintentional dissemination of PII via electronic means operation of the EBS capability suite. Generally, this includes the risk of account hacking, improper permissions set on CWE documents (allowing open access to all), and not locking computers before leaving desks while logged in to the CWE. There are security measures in place involving the WPAFB network, which leverages enclave-level security measures including role-based permission schemes which mitigate the risk of unauthorized disclosure. It is possible that an electronic document may be inadvertently copied to a location that is open to those who should not have access. While the probability of occurrence is low, it remains a risk.

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. The PII is shared internally to Air Force personnel only, and the information is restricted to the participants and managers of the relevant processes.

☐ **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.

Individuals cannot object to collection of the information. Information is used for the performance reporting procedures and awards processing mandated by Air Force instruction (AFI 36-2803).

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.

Consent is not obtained in the normal course of performance reporting and awards processing. Performance reporting and data gathering in support of performance reporting is mandated by Air Force instruction 36-2803 with no regard for unique consent requests.

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.	A privacy Act Statement is provided on the official forms completed by performance reviewers and rating providers involved with performance reporting. Delivery of this statement is electronic by default, or written if the form is printed. The scanned RDP-DECOR6 Air Force form that is uploaded into EBS CWE has "Personal Data - Privacy Act of 1974" specified in the heading of each page. Each CWE site collection offers a "Privacy Policy" link at the bottom of the primary site page. Clicking on the link transitions the user to the Enterprise Information Management (EIM) Privacy Policy web page containing the US Government Information System privacy policy approved for Air Force EIM implementations. The exact text of the privacy policy follows: You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose. This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy. Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details. Linking Policy: The appearance of hyperlinks does not constitute endorsement by the U.S. Air Force of this Web site or the information, products, or services contained therein. For other than authorized activities such as military exchanges and morale, welfare and recreation sites, the U.S. Air Force does not exercise any editorial control over the information you may find at these locations. Such links provided are consistent with the stated purpose of this DoD Web site.

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.