PRIVACY IMPACT ASSESSMENT (PIA)

For the

Contribution-Based Compensation System Software (C2S2)
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: 1849
- ☐ **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 007-57-01-26-01-3196-00

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 PCQ, OPM/GOV'T 1, FO36 SAF AA 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, Security of the Air Force: Powers and duties; delegation by.
10 U.S.C. 265, polices and regulations: 275, Personnel record; 278, Dissemination of information;279, Training Reports.
5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and E.O. 9397, 9830, and 12107.
Air Force Manual 30-3, Volume I-V, Mechanized Personnel Procedures, Air Force Manual 30-130, Base Level Military Personnel System, and Air Force Manual 300-4, Standard Data Elements and Codes; 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 Contribution-Based Compensation System (CCS) provides an effective, efficient, and flexible method for assessing, compensating, and managing the laboratory demo workforce in a fair and equitable manner. CCS represents a substantial philosophical and operational change that goes beyond the traditional performance-based personnel management system. CCS is designed to assist AFRL in achieving the optimal workforce by enhancing workforce competency, quality, and morale, as well as compensating personnel according to their mission contributions. PII information contained in C2S2 is employee name, duty location, salary, social security number, assessments/appraisal, and Statement of Duties and Experience,

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

The privacy risks of PII collected by C2S2 stem from unauthorized disclosure or access of PII data. The risks are addressed through multi-layered and concurrent security mechanisms as follows:
1) The C2S2 application web site is secured behind the AFRL firewall and not publicly accessible.
2) The application web server is configured to respond only to HTTPS SSL-encrypted connections.
3) The application is CAC-enabled and requires all users to present valid CAC certificates.
4) C2S2 requires application-specific user names and passwords for authentication from each of its users. The application enforces a strong password policy.
5) The application strictly limits the use and display of PII data such as SSN except where absolutely necessary.
6) The application limits access to data by a user's application role and organization affiliation so that each user has access only to data as needed.
7) The system administrators follow all DoD and USAF policies and procedures, USAF- and AFRL-issued NOTAMs and other technical security bulletins that pertain to the application systems and software, and apply vendor-provided security patches in a timely manner to maintain the security of application's web and database 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. Defense Civilian Personnel Data System

☐ **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.

Individuals may object to the collection and maintenance of PII information IAW Contesting Record procedures described in the Systems of Records Notices used as authority to maintain the system.

(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.

Personnel have authorized use of this information IAW the Systems of Records Notice used as authority to maintain the system.

(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.

Privacy Act Statement

Authority: 10 U.S.C. 8013, Security of the Air Force: Powers and duties; delegation by. 10 U.S.C. 265, polices and regulations: 275, Personnel record; 278, Dissemination of information;279, Training Reports. 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and E.O. 9397, 9830, and 12107. Air Force Manual 30-3, Volume I-V, Mechanized Personnel Procedures, Air Force Manual 30-130, Base Level Military Personnel System, and Air Force Manual 300-4, Standard Data Elements and Codes; and E.O. 9397 (SSN).

Purpose: To provide data to the Defense Civilian Personnel Data System and the Defense Finance Accounting System to compensate personnel according to their yearly contribution score based upon the results of the Contribution-Based Compensation System.

Routine Uses: None

Disclosure: Voluntary. Failure to provide the PII information would result in employee not being compensated.

The following banner is posted when logging into the C2S2 database.

"*** GOVERNMENT WARNING ***

The security accreditation level of this Department of Defense system allows for handling of data that is Unclassified For Official Use Only and below. Do not use this web site to process, store, or transmit any information classified above the accreditation level of this system.

"This site is intended for the use of the Air Force Research Laboratory only. Do not reproduce or distribute the content of this site to a wider audience without coordination with the information owner and your unit public affairs office.

"This is a Department of Defense computer system. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

"The appearance of hyperlinks to other sites 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 are provided 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.