PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Security Enterprise Communication & User Reporting Environment (SECURE) Foreign Travel/Foreign Contact

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

02/08/21

Air Force Materiel Command

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [x] From Federal employees and/or Federal contractors
- [ ] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [ ] New DoD Information System
- [x] New Electronic Collection
- [ ] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

Provide an enterprise-level framework to automate and support security related activities and processes, including foreign travel requests and foreign contact information. Information collected includes identification, contact, and security-related data, citizenship, employment information, home/cell phone, mailing/home address, official duty address, passport information, place of birth, work email address, birth date, official duty telephone number, position/title, rank/grade, security information, emergency contact, names, social security number, visa number, issuing country, naturalization certificate number, naturalization date, other citizenship, US clearance information, NATO, special access program information, and SCI information.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

PII is collected to populate required fields in existing official paper and electronic forms and documents. The PII is intended to identify users and associate them with their instances of foreign travel and foreign contact.

e. Do individuals have the opportunity to object to the collection of their PII? [x] Yes [ ] No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

SECURE is not the initial point of PII collection. The individuals on whom the PII will be collected have already given voluntary responses to information requested by official questionnaires (e.g., SF 86 Questionnaire for National Security Positions) that include full name, former names and aliases; date and place of birth; social security number (SSN); hair and eye color; biometric information; gender; mother's maiden name; DoD identification number; current and former home and work addresses, phone numbers and email addresses; employment history; military record information; education and degrees earned; names of associates and references with their contact information; passport information; citizenship; criminal history; civil court actions; prior security clearance and investigative information; behavioral/mental health history; records related to drug and/or alcohol use; financial record information; credit reports; the name and marriage information for current and former spouse(s); the citizenship, name, date and place of birth, and addresses for all relatives. Individuals can object to the collection of PII on the questionnaires by declining to complete the initial questionnaire. If an individual chooses not to supply the requested information, they may be in jeopardy of losing their national security position which requires continuous evaluation and monitoring.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [ ] Yes [x] 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.

As described above, PII data in the system is primarily is provided voluntarily by individuals as part of authorized data collections. Specific uses of the collected data are described in the Privacy Act statements on the data collection forms. The data collected is used to determine

risks to national security that may be associated with foreign travel and foreign contacts and for continuous evaluation of covered individuals to maintain eligibility to hold sensitive positions. Covered individuals incur a continuing security obligation to be aware of the risks associated with foreign intelligence operations and/or possible terrorist activities directed against them in the U.S. and abroad, and to be aware they possess or have access to information that is highly sought after by our foreign adversaries and competitors. The reporting enables collection and proper preparation before and reporting after foreign travel. The data collected may further be used in with an inquiry by a DoD component or components which may or may not lead to further inquiries and /or investigation.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

☒ Privacy Act Statement ☒ Privacy Advisory ☐ Not Applicable

Privacy Advisory– Any misuse or unauthorized disclosure may result in either civil or criminal penalties. Information you provide is protected by the Privacy Act of 1974, U.S.C. Your responses to these questions are intended to aid security personnel in determining your eligibility to information protected under Executive Order 13526. Privacy Act Statement:

Authority: The Department of Defense is authorized to ask these questions under Executive Orders 10450, 10865,12333, 12968 and 13467; sections 3301, 3302, and 9101 of Title 5, United States Code (U.S.C.); sections 2165 and 2201 of Title 42, U.S.C.; chapter 23 of Title 50, U.S.C; and parts 2, 5, 731, 732, 736 of Title 5, Code of Federal Regulations (CFR).

ROUTINE USES: Serves to report all foreign travel and reportable foreign contact by those who hold national security positions to the cognizant security official(s) and counterintelligence officials. Also serves as a record of foreign travel and foreign contact reports. Records will be transmitted to the Defense Information System for Security (or successor system) for personnel vetting actions and maintained in this system for the duration individual holds a national security position. Disclosed data is subject to review by cognizant security and counterintelligence officials. Furthermore, records maybe disclosed to appropriate agencies, entities and persons when a breach is suspected or confirmed; or when disclosure is necessary to respond to suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Disclosure: Voluntary; However, failure to disclose the information may result in forfeiture of eligibility to hold the national security position.

SORN: DUSDI 02-DoD

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒ Within the DoD Component	Specify.	Security personnel and supervisors of individuals covered by the system including AF Office of Special Investigations and AF Insider Threat Office (within SECURE and via submission to DISS and NBIS integration)
☒ Other DoD Components	Specify.	Other DoD agencies on an as needed basis to counter foreign intelligence, counterintelligence and insider threat (through manual reporting channels, as necessary)
☒ Other Federal Agencies	Specify.	Other federal agencies on an as needed basis to counter foreign intelligence, counterintelligence and insider threat (through manual reporting channels, as necessary)
☐ State and Local Agencies	Specify.	
☐ Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	
☐ Other *(e.g., commercial providers, colleges).*	Specify.	

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

☒ Individuals ☐ Databases

☐ Existing DoD Information Systems ☐ Commercial Systems

☐ Other Federal Information Systems

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

- [ ] E-mail
- [ ] Official Form (*Enter Form Number(s) in the box below)*
- [ ] Face-to-Face Contact
- [ ] Paper
- [ ] Fax
- [ ] Telephone Interview
- [ ] Information Sharing - System to System
- [x] Website/E-Form
- [ ] Other *(If Other, enter the information in the box below)*

users enter their own information

k. 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 must be consistent.

- [x] Yes
- [ ] No

If "Yes," enter SORN System Identifier DUSDI 02-DoD

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. N1-AFU-89-25

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

T 31 - 08 R 22.00 - Foreign Travel -- Destroy after 5 years.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

Executive Orders: 10450 -- Security requirements for Government Employment; 10865 -- Safeguarding classified information; 12333 -- United States Intelligence Activities; 12968 -- Access to Classified Information; 13526 -- Classified National Security Information; 13467 -- Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information;
sections 3301, 3302, and 9101 of Title 5, United States Code (U.S.C.);
sections 2165 and 2201 of Title 42, U.S.C.;
chapter 23 of Title 50, U.S.C;
and parts 2, 5, 731, 732, 736 of Title 5, Code of Federal Regulations (CFR).

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☒ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

this application does not collect PII from members of the public

NOTE: Sections 1 above is 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 if they contain information that would reveal sensitive information or raise security concerns.