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:

Department of Defense Secure Access File Exchange (DoD SAFE)

2. DOD COMPONENT NAME:

Defense Information Systems Agency

3. PIA APPROVAL DATE:

07/02/24

SD5 Enterprise Services

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

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

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

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] 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.

Department of Defense Secure Access File Exchange (DoD SAFE):
Designed for securely exchanging various types of electronic files. DoD SAFE is for "UNCLASSIFIED USE ONLY". DoD SAFE is a web based tool to provide DoD Common Access Card (CAC) users the capability to send/receive files up to 8GB. The DoD community (civilian, military, and contractors) who possess a valid CAC are the intended target audience. Accessibility and authentication to use DoD SAFE is handled via web browser, email, and CAC. DoD SAFE is approved for the transfer of up to "CONTROLLED UNCLASSIFIED INFORMATION" (CUI) in any format.

CAC-Authenticated Users can perform (a) file pick-ups, (b) file drop-offs TO, and (c) request drop-offs FROM both CAC and non-CAC holders. During drop-off, Authenticated User must provide both Sender and Recipient's name and email addresses.

Unauthenticated Users are limited to the ability to perform (a) file pick-ups and (b) file drop-off in response to an Authenticated Users drop-off request. For drop-off, Unauthenticated User is limited to sending file back to only the originating Authenticated User's email.

PII Data collected during Authentication (from IdSS): EDIPI, Email, Common Name, & Organization
PII Data collected during Authenticated Users' drop-off and/or drop-off request: Name, & Email

The type of PII that is collected includes: Name(s), DoD ID Number, Work Email Address and Personal Email Address.

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)*

DoD SAFE collects PII to facilitate and leverage the Identity Synchronization Service (IdSS), which is used to identify authorized users and PII that facilitates the transfer and sharing of files through data exchange such as personal and work email addresses.

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.

Individuals can object to the collection of their PII by not completing and submitting the information required.

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

Individuals can object to the specific uses of their PII by not completing and submitting the information required.

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

Banner across all DOD SAFE pages: "This information system is approved for CUI and PII/PHI data."

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

☒	Within the DoD Component	Specify.	DISA
☒	Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	All DoD Components
☒	Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	All Federal Information Systems
☐	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.	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.
☐	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

Existing DoD Information System: Identity Synchronization Service (IdSS)

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)*

☐ In-Person Contact ☐ Paper

☐ Fax ☐ Telephone Interview

☒ Information Sharing - System to System ☒ Website/E-Form

☐ Other *(If Other, enter the information in the box below)*

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.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier K890.14

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. DAA-GRS2017-0003-0001: GRS 5.2: Item: 010

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

(3) Retention Instructions.

Schedule Subject: GRS 5.2: Transitory and Intermediary Records

This schedule covers records of a transitory or intermediary nature. Transitory records are routine records of short term value (generally less than 180 days).

NARA Job Number: DAA-GRS2017-0003-0001
-GRS 5.2 Item 010: Transitory Records: Temporary. Transitory records are routine records of short term value (generally less than 180 days). Destroy when no longer needed for business use, or according to agency predetermined time period or business rule.

NARA Job Number: DAA-GRS2017-0003-0002
-GRS 5.2 Item 020: Intermediary Records: Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

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.

The following authority allows Department of Defense Secure Access File Exchange (DoD SAFE) to collect the following data:
-10 U.S.C. Chapter 8; 000 Directive 5105.19
-DoD Directive 1000.25 DoD Personnel Identity Protection (PIP) Program
-DoD Enterprise User Data Management Plan for Persons and Personas, Aug 11, 2010
Executive Order 10450 National Archives;
Public Law 99-474, the Computer Fraud and Abuse Act;
Public Law 114-328, National Defense Authorization Act for Fiscal Year 2017, Section 1653
DoD Directive 5105.19, Defense Information Systems Agency
DoD Directive 5400.11 R Department of Defense Privacy Program
DoDI 8910.01 Vol. 2, DoD information Collection Manual: Procedure for DoD Public Information Collections
DoDI 8510.01, Risk Management Framework (RMF) for DoD IT

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.

OMB Control Number: 0704-0415
Expiration Date: None