

## 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 Safe Access File Exchange (DoD SAFE)

**2. DOD COMPONENT NAME:**

Defense Information Systems Agency

**3. PIA APPROVAL DATE:**

08/25/23

### 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.)

- |  |  |
|--|--|
| <input checked="" type="checkbox"/> From members of the general public                 | <input type="checkbox"/> From Federal employees                          |
| <input type="checkbox"/> from both members of the general public and Federal employees | <input type="checkbox"/> Not Collected (if checked proceed to Section 4) |

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

- |  |   |
|--|---|
| <input type="checkbox"/> New DoD Information System                    | <input type="checkbox"/> New Electronic Collection      |
| <input checked="" type="checkbox"/> Existing DoD Information System    | <input type="checkbox"/> Existing Electronic Collection |
| <input type="checkbox"/> 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.**

**IMPORTANT NOTE:** The Department of Defense Safe Access File Exchange (DoD SAFE) capability is uniquely accredited under the Defense Collaboration Service (DCS) accreditation Authority to Operate (ATO). This PIA represents the symbolic accreditation relationship of the referenced capabilities.

DoD-SAFE (Department of Defense Safe Access File Exchange):

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 large files up to 8GB. The DoD community (civilians, military, and contractors) who possess a valid CAC are the intended target audience for this iteration of DoD SAFE. Accessibility and authentication to use DoD SAFE is handled via email and CAC. The aforementioned DoD SAFE user community will have the capability to send files to person(s) where their email address resides within the parameters of .mil. All file transfers via DoD SAFE must be UNCLASSIFIED official US Government related business. DoD SAFE is approved for the transfer of "CONTROLLED UNCLASSIFIED INFORMATION" (CUI) in any format.

Authorized Users:

Only authorized DoD CAC users will be able to login and utilize DoD SAFE. However, non-registered non-DoD users may access the system to pick up files from or drop off files to DoD CAC users.

PII Collected Data:

DoD SAFE collects only business PII 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. Transfer files/packages may also contain individual PII or PII groupings information.

DoD SAFE users must register with their DoD CAC. Individuals wanting to send files/packages via DoD SAFE must provide the following:

- Name (sender and recipient)
- Email Address (sender and recipient)
- Sender data (may contain PII or subset of PII, which sender may knowingly or unknowing upload to platform).

**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. Transfer files/packages may also contain individual PII or PII groupings information. DoD SAFE is approved for the transfer of "UNCLASSIFIED" files in any format to include CUI, which may contain PII that may have been collected via another method (i.e. another source system). Refer to

Section 1 (i) (k).

e. Do individuals have the opportunity to object to the collection of their PII?  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.

DoD Government individuals (civilian, military, and contractor) have the opportunity to object to the collection of their PII. However, the objecting individual will not be granted authorization to utilize the DoD SAFE application. Any specific PII, which may be collected via other methods by which individuals are allowed to give or withhold their consent.

f. 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.

DoD SAFE: DoD SAFE is only a means for data transfer.

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

Green global banner across the top of the DoD SAFE screen states: 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. All Federal Information Systems

Other DoD Components (i.e. Army, Navy, Air Force) Specify. All Federal Information Systems

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. All Federal Information Systems

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://dpclid.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.

**I. 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-  
GRS2017-0003-0002:GRS 5.2: Item: 020

(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 statute 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.

-5 U.S.C. 301. Departmental Regulation

-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

**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 approval is not required in accordance with Section 8.b.11 of Enclosure 3 of DoD Manual 8910.01 - Volume 2.