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:

Defense Collaboration Service (DCS)/Department of Defense Safe Access File Exchange(DOD SAFE)

2. DOD COMPONENT NAME:

Defense Information Systems Agency

Enterprise Collaboration Services Portfolio Management Office

3. PIA APPROVAL DATE:

3/16/2022

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
- ☐ 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
- ☐ 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.

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 symbiotic accreditation relationship of DCS and DoD SAFE. PII (Personal Identifiable Information) data elements collected are as follows: Protected Health Information (PHI), employment information, work email address, personal email address, names, and DoD ID Number (Refer to Section 2(a)).

DCS (Defense Collaboration Service):
Allows users to collaborate on-line using web conference and chat capabilities. Web conferencing includes audio, video, document presentation, visible notes, instant messaging publicly or privately and transcription. The content uploaded and displayed is at the discretion of the moderator. All DCS administrators and moderators utilize PKI for authentication.

A DCS administrator and a DCS moderator have the ability to create, host, and permit access to web conferences. A DCS user can be authenticated (have PKI credentials) or a non-authenticated (guest).

****

DoD-SAFE (Department of Defense Safe Access File Exchange):
Designed for securely exchanging various types of electronic files. DoD SAFE is for "UNCLASSIFED 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) whom 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) whom the email address resides within the parameters of .mil. All file transfers via DoD SAFE must be UNCLASSFIED official US Government related business. DoD SAFE is approved for the transfer of "CONTROLLED UNCLASSIFED INFORMATION" (CUI) in any format.

Authorized Users:
Only authorized DoD CAC users will be able to login and utilize DoD SAFE.

PII Collected Data:
DoD SAFE does not collect individual PII or PII groupings (unique identifiers) but does facilitate the transfer and sharing of files through data exchange. Such files/packages may 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 knowing 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)*

DCS PII collected is used to authenticate a DCS Administrator, moderator or authenticated users.

****

DoD SAFE: Approved for the transfer of "UNCLASSIFED" files in any format to include CUI, which may contain PII that may have been collected via another method (i.e. another source system).

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.

DCS: If an individual, with a PKI certificate, objects to the collection of their PII they can select [Cancel] when prompted at the certificate selection pop up and join a web conference as a guest. Non-authenticated users join web conferences as guests automatically, although they must agree to the "User Acceptance Agreement" at the "US Department of Defense Warning Statement" prompt.

****

DoD SAFE: DoD Government individuals (civilian, military, and contractor) who are sending files via DoD SAFE have the opportunity to object to the collection of their PII. The objecting individual will not be granted authorization to utilize the DoD SAFE application. However, file recipients will not have the opportunity to object to their PII information being submitted to DoD SAFE for file drop off.

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.

DCS: Only information used for authentication is collected. The use of the ID information is integral to the function of DCS. A profile cannot be created with ID information.

****

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

DCS: Red global banner across the top of the DCS screen states: This information system is approved for "SECRET" data. Default information/slide displayed when all DCS sessions are started states: *PII/PHI UPDATE*PII and PHI are allowed on the DCS system as long as the meeting is "NOT recorded" and "NOT written in the chat panel".

DCS Security Disclaimer: DCS is not approved for recording of PII and PHI information as identified in NISTSP 800-53, DoD 5400.11-R Department of Defense Privacy Program and DoD 6025.18-R DoD Health Information Privacy Regulation. For further reference please review these documents along with the Privacy Act and Health Insurance Portability and Accountability Act Core training document created by Tricare.

****

DoD SAFE: 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 exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

[X]	Within the DoD Component	Specify.	All Federal Information Systems
[X]	Other DoD Components	Specify.	All Federal Information Systems
[X]	Other Federal Agencies	Specify.	All Federal Information Systems
[ ]	State and Local Agencies	Specify.	
[X]	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.
[X]	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
- [X] Existing DoD Information Systems
- [ ] Other Federal Information Systems
- [ ] Databases
- [ ] Commercial Systems

DMDC Identity Management System

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

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

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 [X] No

If "Yes," enter SORN System Identifier

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.

DoD SAFE is not a system of record and is only approved for the transfer of UNCLASSIFIED files in any format to include CUI. Information about an individual cannot be retrieved by the individuals name or other unique identifier.

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 & DAA-GRS2017-0003-0002

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

(3) Retention Instructions.

DCS:
General Records Schedule 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).
- GRS 5.2 Item10: Transitory Records: Temporary. Destroy when no longer needed for business use, or according to agency predetermined time period or business rule
- GRS 5.2 Item 20: 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.

****

DoD SAFE:
Not applicable. Does not contain records.

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.

-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.

DoD SAFE is a file transfer/exchange system. In accordance with DoD Manual 8910.01 VOL2, "DoD Information Collections Manual: Procedures for DoD Public Information Collections Enclosure 3, Section 1a." DoD SAFE is not a public information collections, which requires the solicitation of responses from members of the public. Therefore, DoD SAFE is not subject to OMB review or requires an OMB control number.