

## 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)

**2. DOD COMPONENT NAME:**

Defense Information Systems Agency

**3. PIA APPROVAL DATE:**

07/20/20

SD3 Enterprise Wide Services Portfolio Office

### SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

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

- |   |   |
|---|---|
| <input type="checkbox"/> From members of the general public   | <input checked="" type="checkbox"/> From Federal employees and/or Federal contractors |
| <input type="checkbox"/> From both members of the general public and Federal employees and/or Federal contractors | <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.**

DCS 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 use 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).

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

**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.

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.

**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.

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.

**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.)

- |  |  |   |
|--|--|---|
| <input type="checkbox"/> Privacy Act Statement | <input checked="" type="checkbox"/> Privacy Advisory | <input type="checkbox"/> Not Applicable |
|--|--|---|

Green global banner across the top of the DCS screen states: This information system is approved for UNCLASSIFIED//FOUO and PII/PHI data

Default information/slide displayed when all DCS sessions are started states:

\*PII/PHI UPDATE\* PII and PHI are now allowed on the DCS system as long as the meeting is NOT recorded and NOT written in the chat

panel.

Security Disclaimer: DCS is not approved for recording of PU 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.

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

- |   |  |
|---|--|
| <input checked="" type="checkbox"/> Within the DoD Component  | Specify. DISA  |
| <input type="checkbox"/> Other DoD Components   | Specify.   |
| <input type="checkbox"/> Other Federal Agencies   | Specify.   |
| <input type="checkbox"/> State and Local Agencies   | Specify.   |
| <input checked="" type="checkbox"/> 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. Booze Allen Hamilton - 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. |
| <input type="checkbox"/> 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)**

- |  |   |
|--|---|
| <input type="checkbox"/> Individuals                                 | <input type="checkbox"/> Databases          |
| <input checked="" type="checkbox"/> Existing DoD Information Systems | <input type="checkbox"/> Commercial Systems |
| <input type="checkbox"/> Other Federal Information Systems           |   |

DMDC Identity Management System

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

- |   |  |
|---|--|
| <input type="checkbox"/> E-mail   | <input type="checkbox"/> Official Form (Enter Form Number(s) in the box below) |
| <input type="checkbox"/> Face-to-Face Contact                                     | <input type="checkbox"/> Paper   |
| <input type="checkbox"/> Fax  | <input type="checkbox"/> Telephone Interview                                   |
| <input checked="" type="checkbox"/> Information Sharing - System to System        | <input type="checkbox"/> Website/E-Form  |
| <input type="checkbox"/> 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    DMDC.02 DoD

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.

**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.    GRS 5.1 Item 010

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

(3) Retention Instructions.

Disposition Authority DAA-GRS2016-0016-0001 Temporary. Destroy when business use ceases.

**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 Personnas, 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.