

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 User Registration System (DURS) Records DTIC 01

2. DOD COMPONENT NAME:

Defense Technical Information Center

3. PIA APPROVAL DATE:

03/18/19

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.

To collect registration requests, validate eligibility, and maintain an official registry that identifies individuals who apply for, and are granted access privileges to DTIC owned or controlled computers, databases, products, services, and electronic information systems. Name; DoD Identification (ID) Number; citizenship; service type; personnel category; civilian pay grade; military rank; organization/company name; office mailing address/physical location; office email address; userid and password/reset questions; office telephone number(s); access eligibility; dissemination/distribution group codes; and personal and facility security clearance level(s). Records also contain the government approving official's name, office phone number and email address; date of registration activation; and the projected date of expiration. Where applicable, the records contain contract number(s), contract expiration date(s), and the Militarily Critical Technical Data Agreement (MCTDA) Certification Number.

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)

Identification and verification of each individual's eligibility for authorized access to DTIC's controlled S&T collections and suite of services according to specific roles, e.g., Department of Defense (DoD) military and civilian personnel, other U.S. Federal Government personnel, their contractors and grantees.

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.

The information is required to establish the user account/profile and provide access to DTIC's controlled scientific and technical collection. Personal information is collected through the synchronization service by existing DoD and federal systems, DMDC and OPM, as well as from manual customer input/registration. Users are prompted to consent before entering the U.S. Government Information System and to read and agree to the terms of agreement for the collection of information prior to the registration process. The Privacy Act Statement on the registration site includes the following: DISCLOSURE: Voluntary, but failure to provide the requested personal information may prevent the individual from gaining access to DTIC's controlled information services.

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.

DTIC's automated systems involves matching a user profile against the metadata describing a controlled information asset. Information submitted at registration is used to authenticate user privileges with specific classes of controlled content.

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

DTIC informs individuals with the following Privacy Act Statement posted on the DTIC Registration Website, and users must agree to the terms in order to proceed:

Privacy Act Statement:

AUTHORITY: E.O. 13526, Classified National Security Information; DoD Directive (DoDD) 5105.73 Defense Technical Information Center (DTIC); DoD Instruction (DoDI) 3200.12 DoD Scientific and Technical Information Program (STIP); DoD Manual (DoDM) 3200.14, Volume 1, Principles and Operational Parameters of the DoD Scientific and Technical Information Program (STIP): General Processes; DoDD 5230.25 Withholding of Unclassified Technical Data from Public Disclosure.

PURPOSE: To identify individuals who apply for, and are granted, access privileges to DTIC products and electronic information systems.

ROUTINE USE(S): Routine uses are listed in the applicable system of records notice Defense User Registration System (DURS) Records DTIC 01. <https://dpcl.d.defense.gov/Portals/49/Documents/Privacy/SORNs/OSDJS/DTIC-01.pdf>

DISCLOSURE: Voluntary, but failure to provide the requested personal information may prevent the individual from gaining access to DTIC's controlled information services.

Also, a standard notice is posted on the DTIC site advising individuals that they are accessing a U.S. Government Information System, and they must consent to the posted User Agreement in order to proceed. The Standard Mandatory Notice and Consent Provision for all DoD Information System Agreements itemizes the applicable conditions of use for an information system.

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.
- Other DoD Components Specify.
- Other Federal Agencies Specify.
- 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

Individual, existing DoD information systems (DMDC DPS), and existing Federal information systems electronic Official Personnel Folder (eOPF).

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 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

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

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

(3) Retention Instructions.

Electronic records to be deleted when DTIC determines they are no longer needed for administrative, audit, legal, or operational purposes.

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.

E.O. 13526, Classified National Security Information;
DoD Directive (DoDD) 5105.73 Defense Technical Information Center (DTIC);
DoD Instruction (DoDI) 3200.12 DoD Scientific and Technical Information (STI) Program (STIP);
DoD Manual (DoDM) 3200.14-Volume 1 Principles and Operational Parameters of the DoD Scientific and Technical Information Program (STIP): General Processes.
DoDD 5230.25 Withholding of Unclassified Technical Data from Public Disclosure.

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: 0704-0546

Expiration Date: 31 December 2021