PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense User Registration System
Defense Technical Information Center (DTIC)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐	**New DoD Information System**	☐	**New Electronic Collection**
☒	**Existing DoD Information System**	☐	**Existing Electronic Collection**
☐	**Significantly Modified DoD Information System**		

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒	**Yes, DITPR**	Enter DITPR System Identification Number	4300
☒	**Yes, SIPRNET**	Enter SIPRNET Identification Number	17704
☐	**No**		

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☐ **Yes** ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier DTIC 01

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an 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**

Enter OMB Control Number	0704-0546
Enter Expiration Date	11/30/2018

☐ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

Authority for maintenance of the system:
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;

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The purpose of this system is 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 databases, products, services, and electronic information systems on the NIPRNet and SIPRNet. DTIC utilizes the Defense Manpower Data Center (DMDC) and Office of Personnel Management (OPM) for the purposes of Identity Access Management that provides the infrastructure to leverage authoritative information for personnel digital identity. The records contain the individual's name; DoD identification (ID) number; citizenship; service type; personnel category; civilian pay grade; military rank; organization/ company name; office mailing address/physical location; email office 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; dates 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.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The risks associated with the collected PII contained within the local registration database are low. Records are maintained in secure, limited access, and monitored areas. Database is monitored; authorized access is password protected and common access card (CAC) enabled. Physical entry by unauthorized persons is restricted through the use of locks, guards, passwords, and/or other security measures. Archived data is stored on compact discs, or magnetic tapes, which are kept in a locked, controlled access area. Risks by other factors are mitigated through the Network "defense-in-depth" methodology to protect not only PII information, but other sensitive DoD scientific and technical information contained within the DTIC repository through the use of multi-layered firewalls, Intrusion Detection System, Secure Socket Layer protocols, Secure Routers, Access Control List, Systems Logs, Common Access Card (CAC) authentications, and files permissions. Restricted system administrators/managers within DTIC are responsible for the prevention of unauthorized disclosure outside official use of this information. Access to personal information is limited to properly trained individuals who have a need to know to perform their official assigned duties.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. Defense Technical Information Center

☒ **Other DoD Components.**

Specify. Naval Criminal Investigative Service, 902nd Military Intelligence Group

☒ **Other Federal Agencies.**

Specify. Federal Bureau of Investigation

☐ **State and Local Agencies.**

Specify.

☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

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

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can 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.

(2) If "No," state the reason why individuals cannot object.

j. 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 system 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 content controlled in accordance with DoDM 5200.01, DoDI 5230.24, and DoDD 5230.25.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ **Privacy Act Statement** ☐ **Privacy Advisory**

☐ **Other** ☐ **None**

Describe each applicable format.

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: 5 U.S.C. 301, Departmental Regulations; 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.
PURPOSE: To identify individuals who apply for, and are granted, access privileges to DTIC products and electronic information systems.
ROUTINE USES: Information is used for the purpose set forth above and may be disclosed outside the DoD pursuant to the "Blanket Routine Uses" set forth at the beginning of the OSD's compilation of Systems of Records Notices.
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.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.