PRIVACY IMPACT ASSESSMENT (PIA)

For the

Scientific & Technical Information Archival & Retrieval System - Unclassified (STARS-U)
Defense Threat Reduction Agency

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	8922 (STARS-U)
☐	**Yes, SIPRNET**	Enter SIPRNET Identification Number	
☐	**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 BIN = 007-5058

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 HDTRA 007 Security Services

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

Enter Expiration Date

☒ **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.

DODI 3200.14, DTRIAC Charter, DODD 5105.62; 5 U.S.C. 301, Departmental Regulations; EO 10450, Security Requirements for Government Employment; EO 12065, National Security Information; The Atomic Energy Act of 1954, Section 145; and EO 9397 (SSN), as amended.

The DTRA is designated as the DoD Executive Agent for sustaining general interest nuclear weapons training expertise. The Defense Threat Reduction University is composed of the Defense Nuclear Weapons School and the Defense Threat Reduction Information Analysis Center (DTRIAC).

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.

DTRIAC is the key Department of Defense (DoD) source of information and analysis on nuclear and conventional weapons-related topics. Sponsored by DTRA, DTRIAC has major reference collections of documents, photographic data, and films, and it can search, retrieve, and perform analyses on DTRA-internal and community-wide nuclear/conventional weapons phenomena, effects and technology matters, and related nuclear/conventional technology transfer applications. The STARS-U application allows authorized users access to the reference collection. The STARS-U system collects e-mail, work address (optional), clearance level, citizenship, and caveats for DoD and Department of Energy (DOE) users to control data access to authorized users.

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

The PII data is only used by the software to control access to library collection materials that contain classification, distribution, and caveat controls. The data is not available in a report and is not available to an end user. The system administrators and developers are the only personnel with access to all PII data. The administrators are DoD 8750 certified, TS/SCI cleared, and limited to four personnel at any given time, as approved by the government system owner. The developers have signed Non-Disclosure (NDA) and Organizational Conflict of Interest (OCI) agreements, and they have taken all DTRA information security and PII training. The application has been certified to DoD Information Assurance Certification and Accreditation Process (DIACAP) certification and accreditation standards, and it has appropriate security controls for a Mission Assurance Category II (MAC II)-classified system.

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.

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **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. None. PII from STARS-U is not exchanged.

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.

Individuals can prevent the collection of their PII in the STARS-U system by not applying for a STARS-U account.

(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.

The PII is necessary to control access to DTRIAC library data. The data is not shared or used outside of the software system. Without the PII data, the user cannot have a STARS-U account. If users do not consent to use of their PII, they will not be issued a STARS-U account.

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.	The PII is sent in a DoD Visit Request to DTRA from the user's security office. The data is not collected by the system automatically, but it is compiled from several sources including the DTRA Secure Access database. Privacy Act Statement will be added to the STARS-U account form stating the collection of PII.

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.