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:

Nuclear Test and Radiological Review, HDTRA 010

2. DOD COMPONENT NAME:

Defense Threat Reduction Agency

3. PIA APPROVAL DATE:

12/03/19

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
- [x] 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
- [x] 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.

The Nuclear Test and Radiological Review (NTRR) program uses the Nuclear Test Participants system of records, which is a comprehensive database containing information about participation and dose information for over 500,000 individuals in United States atmospheric nuclear testing (1945-1962), the military occupation forces of Hiroshima and Nagasaki, Japan (1945-1946), or were prisoners of war in Japan at the conclusion of World War II. The program similarly supports an analogous 50,000 DoD personnel associated with U.S. underground nuclear weapon testing (1951-1992), and 6,000 DoD personnel associated with the radiological clean-up of the Pacific Proving Ground (1960s-1980). The NTRR program has many elements designed to assist military and civilian test participants, to help the Department of Veterans Affairs (VA) and the Department of Justice (DOJ) in responding to claims, and to provide information to organizations responsible for studies concerning the health effects of ionizing radiation. These elements include the following:
(a) Researching participation and establishing a register of DoD participants;
(b) Collecting and analyzing all known sources of recorded dosimetry and radiation data applicable to participants, and reconstructing doses in cases where recorded doses are unavailable or incomplete;
(c) Maintaining a comprehensive database of participation and dose information, along with supporting archival materials and documents;
(d) Conducting an extensive public outreach program to ensure maximum interface with the supported participants;
(e) Maintaining the history of each U.S. atmospheric nuclear weapons test operation;
(f) Supporting studies to determine whether participants experience adverse health effects as a result of their test activities; and
(g) Providing accurate and timely responses to requests for information from incoming inquiries.

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)*

Mission-related work as detailed above section in Section 1c.

e. Do individuals have the opportunity to object to the collection of their PII? [x] 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.

Individuals may object by refusing to consent to DTRA collecting their PII on the DTRA Form 150. However, DTRA receives records from NARA or other federal agencies, which may inadvertently contain PII. There is no mechanism to object to the latter.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [x] 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.

Individuals can give their consent for DTRA to collect their information by signing DTRA Form 150, "Nuclear Test Personnel Review Information Request and Release." DTRA Form 150 states routine uses as disclosure of records permitted outside DoD under 5 U.S.C. 552a(b) (Privacy Act) to the VA, DOJ, and Department of Labor (DOL) for identifying and processing claims by individuals who allege job-related disabilities as a result of participation in nuclear test programs and for litigation actions, Veterans Advisory Board on Dose Reconstruction for the purpose of reviewing and overseeing the DoD Radiation Dose Reconstruction Program audits of dose reconstructions; and to the Department of Health and Human Services, and Vanderbilt University for the purpose of conducting epidemiological studies on the effects of ionizing radiation on participants of nuclear test programs. Additional routine uses are listed in the applicable system of records notice HDTRA 010, Nuclear Test Participants, located at: http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570291/hdtra-010/. The individual's release of information to DTRA is completely voluntary. However, failure to provide the requested information may delay or preclude the potential administration of compensation or benefits from other federal agencies, such as the VA, DOJ, or DOL.

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.)*

[X] Privacy Act Statement [ ] Privacy Advisory [ ] Not Applicable

Authority: Atomic Energy Act of 1954; Radiation Exposure Compensation Act; 42 USC 2013, The Public Health and Welfare; 38 U.S.C. 1112, Presumptions Relating to Certain Diseases and Disabilities; 38 U.S.C. 1154, Consideration to be Accorded Time, Place, and Circumstances of Service; 38 CFR 3.309, Disease Subject to Presumptive Service Connection; 38 CFR 3.311, Claims Based on Exposure to Ionizing Radiation; and E.O. 9397 (SSN), as amended.

Purpose: To assist military and civilian test participants, to help the VA and DOJ in responding to claims, and to provide information to organizations responsible for studies concerning the health effects of ionizing radiation.

Routine Uses:
a. To the VA for the purpose of processing claims by individuals who allege service-connected disabilities as a result of participation in nuclear test programs or military operations, as well as litigation actions.
b. To the DOJ and the Department of Labor (DOL) for the purpose of processing claims by individuals who allege job-related disabilities as a result of participation in nuclear test programs or military operations, and for litigation actions.
c. To the Department of Energy (DOE) for the purpose of identifying DOE employees and DOE contractor personnel who were, or may be in the future, involved in nuclear test programs or military operations, and for DOE's use in processing claims or litigation actions.
d. To the Department of Health & Human Services and Vanderbilt University for the purpose of conducting epidemiological studies on the effects of ionizing radiation on participants of nuclear test programs.
e. To the Veterans Board on Dose Reconstruction for the purpose of aiding officials reviewing and overseeing the DoD Radiation Dose Reconstruction Program.
f. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government when necessary to accomplish an agency function related to this system of records. Information may be released to individuals or their authorized representatives.
g. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.
h. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.
i. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the adjudicator, the DoD official(s) or other agency official(s) representing the DoD determine(s) that the records are relevant and necessary to the proceeding.
j. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. §§ 2904 and 2906.
k. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.
l. To appropriate agencies, entities, and persons when (1) the DoD suspects or has confirmed that there has been a breach of the system of records; (2) the DoD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
m. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

Disclosure: Furnishing this information is voluntary; however, failure to provide the requested information may delay or preclude the potential administration of veteran benefits.

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.	Office of General Counsel
[X] Other DoD Components	Specify.	USA, USN, and USAF Office of The Surgeon Generals
[X] Other Federal Agencies	Specify.	VA, DOJ, Department of Labor, Department of Energy, Department of Health and Human Services, Veterans' Advisory Board on Dose Reconstruction. National Archives and Records Administration and appropriate Federal, foreign, or international law enforcement authority.
[X] State and Local Agencies	Specify.	State, local, territorial, or tribal law enforcement authorities.
[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.	All CACI, Inc. staff, including subcontractors in support of contract HDTRA1-15-C-0002 are required to safeguard to NTRR PII as per FAR privacy clauses i.e. 52.224-1 Privacy Act Notification, 52.224-2 Privacy Act, and 32 CFR 310 DoD Privacy program. As per contract deliverables, A004, all contract staff are required to annually complete Cyber Awareness Challenge, Privacy Act, and Personally Identifiable Information training; and per A008, they are required to sign an NTRR user's agreement and non-disclosure form before gaining access to NTRR PII.
[X] Other *(e.g., commercial providers, colleges).*	Specify.	National Cancer Institute and Vanderbilt University - Atomic veteran radio-epidemiology and/or biodosimetry studies. Principal investigators maintain approved research protocol (via their Institutional Review Board), which includes no public release of Privacy Act data

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

- [X] Individuals
- [ ] Databases
- [ ] Existing DoD Information Systems
- [ ] Commercial Systems
- [ ] Other Federal Information Systems

Information is collected by hard copy (VA, DOJ, DTRA, and veteran correspondence), and by telephone interview.

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

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

DTRA Form 150

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.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier HDTRA 010

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.

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. N1-374-09-04

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

(3) Retention Instructions.

Records will be retained permanently. Retain physical and legal custody at agency for 75 years after case termination then transfer to NARA.

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.

Atomic Energy Act of 1954; Radiation Exposure Compensation Act; 42 USC 2013, The Public Health and Welfare; 38 U.S.C. 1112, Presumptions Relating to Certain Diseases and Disabilities; 38 U.S.C. 1154, Consideration to be Accorded Time, Place, and Circumstances of Service; 38 CFR 3.309, Disease Subject to Presumptive Service Connection; 38 CFR 3.311, Claims Based on Exposure to Ionizing Radiation, and E.O. 9397 (SSN), as amended.

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.

0704-0447 30 November 2020

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)***?** *(Check all that apply)*

☐ Biometrics	☒ Birth Date	☐ Child Information
☐ Citizenship	☐ Disability Information	☒ DoD ID Number
☐ Driver's License	☐ Education Information	☐ Emergency Contact
☐ Employment Information	☐ Financial Information	☒ Gender/Gender Identification
☒ Home/Cell Phone	☐ Law Enforcement Information	☐ Legal Status
☒ Mailing/Home Address	☐ Marital Status	☒ Medical Information
☒ Military Records	☐ Mother's Middle/Maiden Name	☒ Name(s)
☐ Official Duty Address	☐ Official Duty Telephone Phone	☒ Other ID Number
☐ Passport Information	☐ Personal E-mail Address	☐ Photo
☒ Place of Birth	☒ Position/Title	☐ Protected Health Information (PHI)[1]
☐ Race/Ethnicity	☒ Rank/Grade	☐ Religious Preference
☐ Records	☐ Security Information	☒ Social Security Number (SSN) *(Full or in any form)*
☐ Work E-mail Address	☒ If Other, enter the information in the box below	

Dates and extent of test anticipation, radiation exposure data, unit of assignment, and documentation relative to administrative claims, proceedings, or civil litigation.

If the SSN is collected, complete the following questions.

(*DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)*

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

☐ Yes ☒ No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

No, the most recent SSN Justification memo was approved in August 2016. DTRA submitted an updated memo to DPCLTD and is waiting for approval.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

Category 6: The Federal Workers' Compensation Program continues to track individuals through the use of the SSN. As such, systems, processes, or forms that interact with or provide information for the administration of this system or associated systems may be required to retain the SSN. The NTRR Program has many elements designed to assist military and civilian test participants, to help the Department of Veterans Affairs and the Department of Justice in responding to Federal Workers' Compensation Programs.
Category 11 Legacy System Interface: The NTPR program currently operates under legacy systems that utilize SSNs as the primary identifier for government compensation. The requirement for SSNs is from those agencies identified in the acceptable use category 6.

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

SSN data is not printed or included on lists and redacted on documents as appropriate.

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

☒ Yes ☐ No

The NTRR Program collects privacy act information to assist military and civilian test participants and to help VA and DOJ in responding to claims. Personal identification data (name, rank, grade, service number, social security number, date of birth) is used to uniquely identify the individual. This is crucial when dealing with a population of approximately 500,000 personnel. A personal key number is used in place of SSNs as much as possible

b. What is the PII confidentiality impact level[2]? ☒ Low ☐ Moderate ☐ High

[1]The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2]Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- [X] Cipher Locks
- [X] Combination Locks
- [X] Key Cards
- [X] Security Guards
- [X] Closed Circuit TV (CCTV)
- [X] Identification Badges
- [X] Safes
- [ ] If Other, enter the information in the box below

Records are maintained in a controlled facility and entry is restricted by the use of security guards and intrusion alarm systems. Paper records, microfilm/fiche, and computer systems are only accessible by authorized personnel. Access to digital data requires user validation prior to use.

(2) Administrative Controls. *(Check all that apply)*

- [X] Backups Secured Off-site
- [X] Encryption of Backups
- [X] Methods to Ensure Only Authorized Personnel Access to PII
- [X] Periodic Security Audits
- [X] Regular Monitoring of Users' Security Practices
- [X] If Other, enter the information in the box below

Records are limited to person(s) responsible for servicing the record in the performance of their official duties and who are properly screened and cleared for need-to-know.

(3) Technical Controls. *(Check all that apply)*

- [ ] Biometrics
- [X] Command Access Card (CAC)
- [X] DoD Public Key Infrastructure Certificates
- [X] Encryption of Data at Rest
- [X] Encryption of Data in Transit
- [ ] External Certificate Authority Certificates
- [X] Firewall
- [X] Intrusion Detection System (IDS)
- [X] Least Privilege Access
- [X] Role-Based Access Controls
- [ ] Used Only for Privileged (Elevated Roles)
- [X] User Identification and Password
- [X] Virtual Private Network (VPN)
- [ ] If Other, enter the information in the box below

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

Personal information is restricted to specific folders on our digital computer drives and also restricted hard-copy repositories within NTPR spaces.