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:

CDRR - CENTRAL DOSIMETRY RADIATION REPOSITORY

2. DOD COMPONENT NAME:

United States Army

3. PIA APPROVAL DATE:

AMC - AMCOM - U.S. Army Aviation and Missile Command

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees
- [x] from both members of the general public and Federal employees
- [ ] 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.

Personnel radiation exposure readings are archived in the Army's Central Dosimetry Radiation Repository (CDRR), an application reflecting event readings for all Army personnel who are occupationally exposed to ionizing radiation. A web-based application linked to the CDRR satisfies legal requirements specified in 10 CFR 19 and 20 by providing electronic dissemination of monthly, quarterly, and annual personnel exposure reports from the CDRR. By law the Army Radiation Dosimetry Laboratory is required to provide the Nuclear Regulatory Commission Form 5, an annual summary of external and internal radiation exposure. Users of the CDRR are the Army Medical Command and Radiation Safety Officers Army-wide. CDRR inherits accreditation from APMS AITR # DA176346 / TCS RDST_AL_AMC_05 – USATA LABORATORY. CDRR will not be migrating to a cloud environment.

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 is used for identification validation purposes only. The data is is used for mission-related purposes to analyze and monitor individual body radiation exposure levels.

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

Per 10 CFR Part 19 (Notices, Instructions and Reports to Workers: Inspections and Investigations) and Part 20 (Standards for Protection Against Radiation), the Army Radiation Dosimetry Laboratory is required to provide the Nuclear Regulatory Commission Form 5, an annual summary of external and internal radiation exposure.

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

10 CFR Part 19 (Notices, Instructions and Reports to Workers: Inspections and Investigations) and Part 20 (Standards for Protection Against Radiation), the Army Radiation Dosimetry Laboratory is required to provide the Nuclear Regulatory Commission Form 5, an annual summary of external and internal radiation exposure. The information collected is used only for that purpose.

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

Privacy and Security Notice

Thank you for visiting our product and reviewing our privacy policy. Our privacy policy is clear: We will collect no personal information about you when you visit our product unless you choose to provide that information to us.

---

1. This product is provided with controlled access by the U.S. Army Aviation & Missile Command.

2. Information presented on this application / website is considered unclassified information and is accessed by authorized users unless otherwise specified. Use of appropriate byline / photo / image credits is requested.

3. For product management, information is collected for statistical purposes. This government computer system uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas. No user-identifying information is collected for this analysis. The information collected includes the following types of data:

a. Number of Hits for Home Page and Number of Successful Hits for Entire Product
b. Number of User Sessions (from United States and International) and Most Active Countries
c. Most and Least Requested Pages
d. Top Entry and Exit Pages
e. Single Access Pages and Number of Page Views
f. Most Downloaded Files
g. Most Submitted Forms and Scripts
h. Most Active Organizations or Companies that Accessed Product

4. For product security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

5. Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with Army Aviation and Missile Command Records Administration Guidelines. All data collection activities are in strict accordance with DoD Directive 5240.1 (reference(p)).

6. Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1987 and the National Information Infrastructure Protection Act.

7. The appearance of hyperlinks does not constitute endorsement by the Department of Defense, the U.S. Army, AMC, or the Army Aviation and Missile Command of the product or the information, products or services contained therein. For other than authorized activities such as military exchanges and Morale, Welfare, and Recreation products, the Department of Defense or the U.S. Army does not exercise any editorial control over the information you may find at these locations. Such links are provided consistent with the stated purpose of this DoD web site.

8. If you have any questions or comments about the information presented here, please forward them to us using the AMCOM Webmaster page at Contact Webmasters.

Privacy Act Statement

Authority: 10 U.S.C. 3013, Secretary of the Army; 29 U.S.C. Chapter 15, Occupational Safety and Health; Army Regulation 385-10, The Army Safety and Occupational Health Program; Army Regulation 40-5, Preventive Medicine; Army Regulation 40-13, Radiological Advisory Medical Teams; Department of the Army Pamphlet 385-10, The Army Safety and Occupational Health Program; 10 CFR part 19 and 20, Nuclear Regulatory Commission and E.O. 9397 (SSN), as amended.

Principal Purpose: Per 29 U.S.C. Chapter 15, Occupational Safety and Health, the Army Radiation Dosimetry Laboratory is required to provide the Nuclear Regulatory Commission Form 5, an annual summary of external and internal radiation exposure.

Disclosure: Mandated by law.

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

[x]	Within the DoD Component	Specify.	Radiation Safety Officers Army Wide
[ ]	Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	

[X] Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	National Cancer Institute; Center for Disease Control; National Council on National Council on Radiation Protection and Measurement; Department of Veterans Affairs
[ ] 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)*

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

Employee/contractor PII is entered in manually by the system owner. This information is provided by the employee/contractor informally either verbally or collected via paper (not an official form). The radiation levels are collected from the individual's assigned dosimeter badges.

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)*
- [ ] In-Person Contact
- [ ] Paper
- [ ] Fax
- [ ] Telephone Interview
- [ ] Information Sharing - System to System
- [ ] Website/E-Form
- [X] Other *(If Other, enter the information in the box below)*

Collected from dosimeter badges worn by each individual that is exposed to radiation to record radiation exposure levels through dosimetry readers.

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 A0385-10 DASC

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. 385-10k1; 900A/6+ (N1-AU-00-0030)

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

(3) Retention Instructions.

T75. Keep in CFA (CDRR) until no longer needed for conducting business, then retire to RHA/AEA. The RHA/AEA will destroy record when the record is 75 years old.

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.

10 U.S.C. 3013, Secretary of the Army; 29 U.S.C. Chapter 15, Occupational Safety and Health; Army Regulation 385-10, The Army Safety and Occupational Health Program; Army Regulation 40-5, Preventive Medicine; Army Regulation 40-13, Radiological Advisory Medical Teams; Department of the Army Pamphlet 385-10, The Army Safety and Occupational Health Program; 10 CFR part 19 and 20, Nuclear Regulatory Commission 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.

A 60-Day Federal Register Notice (FRN) for the collection published on Wednesday, February 5, 2020. The 60-Day FRN citation is volume 85 number 24 FRN 6533-6534. No comments were received during the 60-Day Comment Period.

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	

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 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.

CDRR SSN Justification Memo will be submitted in conjunction with the submission of this PIA.

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

The applicable acceptable use of collection and use of the SSN is the Other Cases (13), stated in DoDI 1000.30, Reduction of SSN Use within DoD. The CDRR archives comprehensive dosimetry records of all Army personnel and for other personnel who use Army dosimetry services. Records meet the requirements of Title 10 CFR 20.2106 and 20.2110 and Occupational Safety and Health Administration 1910.1096(b)(2)(iii). Army Regulation (AR) 385-10 The Army Safety and Occupational Health Program and Department of the Army Pamphlet (DA PAM) 385-10 The Army Safety and Occupational Health Program specifically authorizes the Army Dosimetry Center the use of SSNs and birth dates as a mechanism to track and archive radiation exposure records for Army personnel. Further, Nuclear Regulatory Commission Title 10 CFR 19.13, Notifications and Reports to Individuals, requires the use of SSNs for radiation exposure related data. This regulation also states that each licensee shall make dose information available to workers as shown in records maintained by the licensee under the provisions of 10 CFR 20.2106. The authorization to collect required information is regulated through DA PAM 385-25, paragraph 13-6i(3)(a). This information collected from the dosimetry readers will be used to fill out NRC Form 5.

(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".

CDRR is protected by the use of Secure Sockets Layer protocol, firewalls, and antivirus software. A logon name/password is required for initial access and registration of Common Access Card. Risks are also addressed by following the Health Insurance Portability and Accountability Act of 1996 guidelines. The PII resides on an accredited restricted network with no email services and no public internet access. There is a low risk of unauthorized access and network breaches.

(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 requirement for the SSN is mandated by law and there is no plan to elimination until laws change. The CDRR archives comprehensive dosimetry records of all Army personnel and for other personnel who use Army dosimetry services. Records meet the requirements of Title 10 CFR 20.2106 and 20.2110 and Occupational Safety and Health Administration 1910.1096(b)(2)(iii). Department of the Army Pamphlet

(DA PAM) 385-10 specifically authorizes the Army Dosimetry Center the use of SSNs and birthdates as a mechanism to track and archive radiation exposure records for Army personnel. Further, Nuclear Regulatory Commission Title 10 CFR 19.13, Notifications and Reports to Individuals, requires the use of SSNs for radiation exposure related data. This regulation also states that each licensee shall make dose information available to workers as shown in records maintained by the licensee under the provisions of 10 CFR 20.2106. The authorization to collect required information is regulated through DA PAM 385-10, paragraph 13-6i(3)(a).

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)*

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

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

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

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

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

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

Due to the level of safeguarding, we believe the risk to individuals privacy is minimal. There is a low risk that information can be accessed by unauthorized users through unauthorized access and network breaches. CDRR is protected by the use of Secure Sockets Layer (SSL) protocol; firewalls; and antivirus software. A logon name/password is required for initial access and registration of CAC. Risks are also addressed by following Health Insurance Portability and Accountability Act (HIPAA) of 1996 guidelines. The PII data resides on a accredited restricted set aside network with no email services and no public internet access. Risks have been addressed by securing the data behind the SBU firewall, implementing role restrictions to the least privilege, posting security and privacy notices, and obtaining an approved Privacy Impact Statement. Additionally, all users are required to complete mandatory Computer Use Security, Information Awareness and Personally Identifiable Information (PII) Handling training.