ADAMS ML080360543

U.S. Nuclear Regulatory Commission

Privacy Impact Assessment

(*Designed to collect the information necessary to make relevant determinations regarding the applicability of the Privacy Act, the Paperwork Reduction Act information collections requirements, and record management requirements.)*

For the

RADIATION EXPOSURE INFORMATION AND REPORTING SYSTEM (REIRS)

(This system is located at and operated by Oak Ridge Associated Universities (ORAU), Oak Ridge, Tennessee, for NRC under a NRC/DOE Lab Agreement.)

Date: January 18, 2008

A. GENERAL SYSTEM INFORMATION

1. Provide brief description of the system:

   REIRS serves as the central repository for all NRC radiation exposure monitoring records that are recorded and reported pursuant to Title 10 of the Code of Federal Regulations Part 20 (10 CFR 20) and Regulatory Guide 8.7.

2. What agency function does it support?

   The central repository is used for the oversight of radiation protection policies and practices at NRC facilities.

3. Describe any modules or subsystems, where relevant, and their functions.

   Module 1: Radiation Exposure Information and Reporting System (REIRS) maintaining occupational exposure records reported by NRC licensees, which includes licensee employees and facility visitors.

   Module 2: Employee Exposure Database System (EEDS) maintaining exposure records for NRC employees monitored by NRC dosimeters. The data are collected and reported to the EEDS by the NRC Regional and Headquarter Radiation Safety Officers (RSO).

4. Points of Contact:

Project Manager	Office/Division/Branch	Telephone
Elijah Dickson	RES/DSA/HEB	301-415-6704
Business Project Manager	Office/Division/Branch	Telephone
Technical Project Manager	Office/Division/Branch	Telephone
Elijah Dickson	RES/DSA/HEB	301-415-6704
Executive Sponsor	Office/Division/Branch	Telephone
Brian Sheron	Office Director	301-415-6641

5. Does this Privacy Impact Assessment (PIA) support a proposed new system or a proposed modification to an existing system?

a. ___ New System ___ Modify Existing System _X_ Other (Explain)

This PIA supports the existing and operating system. No modifications are planned at this time.

b. If modifying an existing system, has a PIA been prepared before?

(1) If yes, provide the date approved and ADAMS accession number.

B. INFORMATION COLLECTED AND MAINTAINED

(These questions are intended to define the scope of the information requested as well as the reasons for its collection. Section 1 should be completed only if information is being collected about individuals. Section 2 should be completed for information being collected that is not about individuals.)

1. **INFORMATION ABOUT INDIVIDUALS**

a. Does this system maintain information about individuals?

Yes.

(1) If yes, what group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public) is the information about?

General public (monitored workers at NRC licensed facilities and visitors) and NRC employees.

b. What information is being maintained in the system about individuals (describe in detail)?

Individual's name, social security number, date of birth, radiation dose received, gender.

c. Is the information being collected from the subject individuals?

No. The records maintained in REIRS are reported officially by the NRC licensees. EEDS records are provided by the NRC Regional and Headquarters RSOs. The information about an individual, other than exposure data, is originally provided by the subject individual.

d. Will the information be collected from 10 or more individuals who are **not** Federal employees?

Yes.

(1) If yes, does the information collection have OMB approval?

Yes.

(a) If yes, indicate the OMB approval number: 3150-0006.

e. Is the information being collected from internal files, databases, or systems?

No.

(1) If yes, identify the files/databases/systems and the information being collected.

f. Is the information being collected from an external source(s)?

Yes.

(1) If yes, what are the source(s) and what type of information is being collected?

REIRS data is reported by NRC licensees. EEDS data are provided by NRC Regional and Headquarters RSOs. Radiation exposure information is submitted to the NRC under 10 CFR 20.2206 in accordance with Regulatory Guide 8.7 reporting requirements.

g. How will this information be verified as current, accurate, and complete?

Records are passed through a validation software application that identifies inconsistencies in format and content from the reporting requirements. A summary of the findings are e-mailed or faxed back to the reporting organization to verify that all records were received as expected, and to alert them to any problems with the submittal. All problems are addressed with the submitter prior to loading of the data into the database. A summary of the findings are e-mailed or faxed back to the reporting organization to verify that all records were received as expected. Total number of records and total collective dose are verified to ensure that all records were included.

h. How will the information be collected (e.g. form, data transfer)?

Records are received in hardcopy (paper) form, electronic media (diskette or CD), and secure web transmittal.

i. What legal authority authorizes the collection of this information?

Title 10 Code of Federal Regulations Part 20.2206

j. What is the purpose for collecting this information?

The database of radiation exposure monitoring records serves the NRC's mission of the oversight of radiation protection practices and procedures at NRC licensees, informs the NRC on the status and trends in radiation exposure, provides a source of data for epidemiologic studies, and is the data source for the NRC's annual report on occupational radiation exposure (NUREG-0713) which disseminates information to management, licensees, international organizations, and the public.

2. INFORMATION NOT ABOUT INDIVIDUALS

a. What type of information will be maintained in this system (describe in detail)?

Commercial nuclear power plant information, such as licensing information, vendor, design, outage and power generation data.

b. What is the source of this information? Will it come from internal agency sources and/or external sources? Explain in detail.

Power generation data is provided by the Idaho National Laboratory under contract with the NRC. Licensee information is provided by NRC's Office of Nuclear Material Safety and Safeguards (NMSS).

c. What is the purpose for collecting this information?

Radiation exposure at nuclear power plants is directly related to power production and outages. Licensee information is necessary to determine whether the licensee is currently active and required to report exposure data.

C. USES OF SYSTEM AND INFORMATION

(These questions will identify the use of the information and the accuracy of the data being used.)

1. Describe all uses made of the information.

   - NUREG-0713, Occupational Radiation Exposure at Commercial Nuclear Power Reactors and Other Facilities
   - NRC Form 4, Cumulative Occupational Dose History
   - NRC Form 5, Occupational Dose Record For A Monitoring Period
   - Analysis, trends in radiation protection
   - Examining the effects of regulations and guidance on radiation protection
   - Epidemiological studies
   - Questions and queries from regulators, licensees, other organizations

2. Is the use of the information both relevant and necessary for the purpose for which the system is designed?

   Yes.

3. Who will ensure the proper use of the information?

   The NRC Project Manager approves and authorizes the use of information contained in the system.

4. Are the data elements described in detail and documented?

   Yes.

   a. If yes, what is the name of the document that contains this information and where is it located?

      System files maintained on the REIRS project directory at Oak Ridge Associated Universities (ORAU).

5. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

   No.

   a. If yes, how will aggregated data be maintained, filed, and utilized?

   b. How will aggregated data be validated for relevance and accuracy?

c. If data are consolidated, what controls protect it from unauthorized access, use, or modification?

6. How will the information be retrieved from the system (be specific)?

The primary keys/units used for retrieval and analysis of records stored in the REIRS database can be done by querying names, social security numbers, licensee name/number, and/or time periods.

7. Will this system provide the capability to identify, locate, and monitor (e.g., track, observe) individuals?

No. Individuals are not tracked and observed. Tracks and maintains occupational radiation exposure over the life time of a monitored individual.

a. If yes, explain.

(1) What controls will be used to prevent unauthorized monitoring?

- The database server has no connection to the internet or networks outside the ORAU internal network.
- Only authorized ORAU personnel working on the REIRS project have access to the database.
- The ORAU network maintains a firewall as well as password protected to prevent unauthorized access to the network.
- The REIRS database server has additional security allowing only project personnel authorized by the Project Manager.
- The REIRS data are maintained in an ORACLE database which enforces additional security measures such as username/password and limited roles for authorized users.

8. Describe the report(s) that will be produced from this system.

- NUREG-0713
- Dose history reports (NRC Form 4)
- Exploratory reports

a. What are the reports used for?

NRC Form 4 dose history reports are generated upon request by the monitored individual or authorized requester. The request must be accompanied by a records release signed by the monitored individual. These reports are used by individuals to document past radiation exposure.

NUREG-0713 is an NRC required annual report.

Exploratory reports can be used to examine dose trends over certain periods not reported in NUREG-0713.

b. Who has access to these reports?

- The individual requesting the dose history (must provide a release signed by the monitored individual)
- The NRC REIRS Project Manager
- The ORAU REIRS Project Manager, records manager, and database manager
- NRC Region and HQ RSOs
- DOE REMS Project Manager (by inter-agency agreement)

D. RECORDS RETENTION AND DISPOSAL

(These questions are intended to establish whether the information contained in this system has been scheduled, or if a determination has been made that a general record schedule can be applied to the information contained in this system. Reference NUREG-0910, "NRC Comprehensive Records Disposition Schedule.")

1. Has a retention schedule for this system been approved by the National Archives and Records Administration (NARA)?

   Yes.

   a. If yes, list the disposition schedule.

      NRC Schedule 2, Part 19, Item 16.

2. Is there a General Records Schedule (GRS) that applies to information in this system?

   No.

   a. If yes, list the disposition schedule.

3. If you answered no to questions 1 and 2, complete NRC Form 637, NRC Electronic Information System Records Scheduling Survey, and submit it with this PIA.

   NRC Form 637 is attached to this PIA.

E. ACCESS TO DATA

1. INTERNAL ACCESS

a. What organizations (offices) will have access to the information in the system?

There is no access to REIRS/EEDS outside of ORAU internal network. Only ORAU REIRS project personnel authorized by the ORAU PM and DOE REMS Project Manager have access.

(1) For what purpose?

N/A

(2) Will access be limited?

N/A.

b. Will other systems share or have access to information in the system?

No other system shares or access information in this system. Data being electronically submitted for REIRS/EEDS is not directly loaded into REIRS/EEDS. It is first received by ORAU REIRS personnel and then loaded into system.

c. How will information be transmitted or disclosed?

Information is transmitted, processed and stored in accordance with Privacy Act and cyber security requirements. Transmittal of information is protected by encryption. NRC is currently examining encryption tools that are acceptable and supported for use in the transmittal of PII data.

Information transmitted to DOE is encrypted using Entrust, which uses a FISMA-compliant encryption algorithm.

d. What controls will prevent the misuse (e.g., unauthorized browsing) of information by those having access?

Access is limited to authorized individuals for specific uses under the scope of work in the contract. Authorized individuals have received Privacy Act training and are aware of their responsibilities and consequences of misuse, which may include civil and criminal penalties.

e. Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes.

(1) If yes, where?

ORAU cyber security documentation and REIRS system documentation are maintained at ORAU Information Systems Department (ISD).

2. **EXTERNAL ACCESS**

a. Will external agencies/organizations/public share or have access to the information in this system?

Yes.

(1) If yes, who.

The Department of Energy REMS Project Manager.

b. What information will be shared/disclosed and for what purpose?

The DOE REMS Project Manager has been authorized to have access to the NRC REIRS data under an inter-agency agreement between NRC and DOE. The REIRS exposure records are used to provide documentation of prior exposure as individuals transfer to the DOE or to a DOE facility, or for epidemiological research.

c. How will this information be transmitted/disclosed?

The information is encrypted using Entrust or other FISMA-compliant encryption and is transmitted via e-mail or other electronic media (e.g., CD) through registered mail.

F. <u>TECHNICAL ACCESS AND SECURITY</u>

1. Describe security controls used to limit access to the system (e.g., passwords). Explain.

- ORAU has received “Authority to Operate” from DOE as a FISMA-compliant enclave. The REIRS database is managed within this enclave.
- ORAU firewall
- ORAU’s internal network cyber security plan
- Username/password required to log in to ORAU network
- The REIRS database server is not connected to external networks
- The REIRS server requires additional authorization within ORAU
- The REIRS database requires another level of authorization to access the data

2. Will the system be accessed or operated at more than one location (site)?

No.

a. If yes, how will consistent use be maintained at all sites?

3. Which user group (e.g., system administrators, project manager, etc.) has access to the system?

- The System Administrator has access to the server for maintenance and backup procedures, does not access data within the database
- The ORAU Project Manager, Records Manager, and Database Manager have access to data in the REIRS database.

4. Will a record of their access to the system be captured?

Yes.

a. If yes, what will be collected?

Windows system logs and Oracle database access logs capture who and when access in the database.

5. Will contractors have access to the system?

Yes, assigned ORAU personnel.

a. If yes, for what purpose?

ORAU maintains and operates the system for NRC under a NRC/DOE Lab Agreement.

Ensure that the following Federal Acquisition Regulation (FAR) clauses are referenced in all contracts/agreements/purchase order where a contractor has access to a Privacy Act system of records to ensure that the wording of the agency contracts/agreements/purchase order make the provisions of the Privacy Act binding on the contractor and his or her employees:

- *52.224-1 Privacy Act Notification.*
- *52.224-2 Privacy Act.*

6. What auditing measures and technical safeguards are in place to prevent misuse of data?

Access is limited to authorized individuals for specific uses under the scope of work in the contract. Authorized individuals have received Privacy Act training and are aware of their responsibilities and consequences of misuse, which may

include civil and criminal penalties. Computer use and access logs are monitored by ORAU ISD.

7. Are the data secured in accordance with FISMA requirements?

   Yes, under DOE, ORAU's Designating Authority gave ORAU the Authority to Operate under full FISMA requirements.

   a. If yes, when was Certification and Accreditation last completed?

      August 2007

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL
(For Use by OIS/IRSD/RFPSB Staff)

System Name: Radiation Exposure Information and Reporting System (REIRS)

Submitting Office: Office of Nuclear Regulatory Research (RES)

A. PRIVACY ACT APPLICABILITY REVIEW

___ Privacy Act is not applicable.

_X_ Privacy Act is applicable. See comments.

Comments:

REIRS is maintained and operated at the Oak Ridge Associated Universities (ORAU), Oak Ridge, Tennessee for the NRC under a NRC/DOE Lab Agreement. This system is considered part of NRC's Privacy Act system of records NRC-27, "Radiation Exposure Information and Reporting System (REIRS) Files.

Reviewer's Name	Title	Date
Sandra S. Northern	Privacy Program Officer	February 15, 2008

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

___ No OMB clearance is needed.

___ OMB clearance is needed.

_X_ Currently has OMB Clearance. Clearance No. 3150-0006

Comments:

The information collection has been approved by OMB and expires on November 30, 2010.

Reviewer's Name	Title	Date
Gregory Trussell	Team Leader	2/8/08

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

___ No record schedule required.

___ Additional information is needed to complete assessment.

___ Needs to be scheduled.

_X_ Existing records retention and disposition schedule covers the system - no modifications needed.

___ Records retention and disposition schedule must be modified to reflect the following:

Comments:

Reviewer's Name	Title	Date
Tracy L. Clark	Records Management Analyst	2/20/08

D. BRANCH CHIEF REVIEW AND CONCURRENCE

___ This IT system **does not** collect, maintain, or disseminate information in identifiable form from or about members of the public.

_X_ This IT system **does** collect, maintain, or disseminate information in identifiable form from or about members of the public.

I concur in the Privacy Act, Information Collections, and Records Management reviews:

/RA/ Date: ***02/20/2008***

Margaret A. Janney, Chief
Records and FOIA/Privacy Services Branch
Information and Records Services Division
Office of Information Services

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: **Dr. Brian Sheron, Director, Office of Nuclear Regulatory Research**	
Name of System: **Radiation Exposure Information and Reporting System (REIRS)**	
Date RFPSB received PIA for review: **February 1, 2008**	Date RFPSB completed PIA review: **February 20, 2008**
Noted Issues: This system is considered part of NRC's Privacy Act system of records NRC-27, Radiation Exposure Information and Reporting System (REIRS) Files.	
Margaret A. Janney, Chief Records and FOIA/Privacy Services Branch Office of Information Services	Signature/Date: ***/RA/*** ***02/20/2008***
Copies of this PIA will be provided to: James C. Corbett, Director Business Process Improvement and Applications Division Office of Information Services Paul Ricketts Senior IT Security Officer (SITSO) FISMA Compliance and Oversight Team Computer Security Office	