SYSTEM NAME AND NUMBER:

Radiation Exposure Information and Reporting System (REIRS) Records—NRC 27.

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

Primary system—Oak Ridge Associated Universities (ORAU), Oak Ridge, Tennessee (or current contractor facility).

Duplicate system—Duplicate systems exist, in part, regarding employee exposure records, with the NRC's Radiation Safety Officers at Regional office locations listed in Addendum 1, Part 2, in the Office of Nuclear Reactor Regulations (NRR), the Office of Nuclear Material Safety and Safeguards (NMSS). The Office of Administration (ADM), NRC, One White Flint North, 11555 Rockville Pike, Rockville, Maryland, maintains the employee dosimeter tracking system.

SYSTEM MANAGER(S):

REIRS Project Manager, Radiation Protection Branch, Division of Systems Analysis, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 7902; 29 U.S.C. 668; 42 U.S.C. 2051, 2073, 2093, 2095, 2111, 2133, 2134, and 2201(o); 10 CFR parts 20 and 34; Executive Order (E.O.) 9397, as amended by E.O. 13478; E.O. 12196, as amended; E.O.13708.

PURPOSE(S) 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. This central repository is used for the oversight of radiation protection policies and practices at NRC-licensed facilities.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals monitored for radiation exposure while employed by or visiting or temporarily assigned to certain NRC-licensed facilities; individuals who are exposed to radiation or radioactive materials in incidents required to be reported under 10 CFR 20.2201-20.2204 and 20.2206 by all NRC licensees; individuals who may have been exposed to radiation or radioactive materials offsite from a facility, plant installation, or other place of use of licensed materials, or in unrestricted areas, as a result of an incident involving byproduct, source, or special nuclear material.

CATEGORIES OF RECORDS IN THE SYSTEM:

These records contain information relating to an individual's name, sex, social security number, birth date, place and period date of exposure; name and license number of individual's employer; name and number of licensee reporting the information; radiation doses or estimates of exposure received during this period, type of radiation, part(s) or organ(s) exposed, and radionuclide(s) involved.

RECORD SOURCE CATEGORIES:

Information in this system of records comes from licensees; the subject individual; the individual's employer; the person in charge of the facility where the individual has been assigned; NRC Form 5, "Occupational Exposure Record for a Monitoring Period," or equivalent, contractor reports, and Radiation Safety Officers.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to the disclosures permitted under subsection (b) of the Privacy Act, the NRC may disclose information contained in this system of records without the consent of the subject individual if the disclosure is compatible with the purpose for which the record was collected under the following routine uses:

a. To provide data to other Federal and State agencies involved in monitoring and/or

evaluating radiation exposure received by individuals as enumerated in the paragraph "Categories of individuals covered by the system;"

b. To return data provided by licensee upon request;

c. A record from this system of records which indicates a violation of civil or criminal law, regulation or order may be referred as a routine use to a Federal, State, local or foreign agency that has authority to investigate, enforce, implement or prosecute such laws. Further, a record from this system of records may be disclosed for civil or criminal law or regulatory enforcement purposes to another agency in response to a written request from that agency's head or an official who has been delegated such authority;

d. A record from this system of records may be disclosed as a routine use to a Federal, State, local, or foreign agency to obtain information relevant to an NRC decision concerning hiring or retaining an employee, letting a contract, or issuing a security clearance, license, grant or other benefit;

e. A record from this system of records may be disclosed as a routine use to a Federal, State, local, or foreign agency requesting a record that is relevant and necessary to its decision on a matter of hiring or retaining an employee, issuing a security clearance, reporting an investigation of an employee, letting a contract, or issuing a license, grant, or other benefit;

f. A record from this system of records may be disclosed as a routine use in the course of discovery; in presenting evidence to a court, magistrate, administrative tribunal, or grand jury or pursuant to a qualifying order from any of those; in alternative dispute resolution proceedings, such as arbitration or mediation; or in the course of settlement negotiations;

g. A record from this system of records may be disclosed as a routine use to a Congressional office from the record of an individual in response to an inquiry from the Congressional office made at the request of that individual;

h. A record from this system of records may be disclosed as a routine use to NRC-paid experts or consultants, and those under contract with the NRC on a "need-to-know" basis for a

purpose within the scope of the pertinent NRC task. This access will be granted to an NRC contractor or employee of such contractor by a system manager only after satisfactory justification has been provided to the system manager;

i. A record from this system of records may be disclosed as a routine use to appropriate agencies, entities, and persons when (1) NRC suspects or has confirmed that there has been a breach of the system of records, (2) NRC has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, NRC (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 NRC efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm; and

j. A record from this system of records may be disclosed as a routine use to another Federal agency or Federal entity, when the NRC 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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are maintained on paper and electronic media. The electronic records maintained in Oak Ridge, TN, are in a centralized database management system that is password protected. Backup tapes of the database are generated and maintained at a secure, off site location for disaster recovery purposes. During the processing and data entry, paper records are temporarily stored in designated business offices that are locked when not in use and are accessible only to authorized personnel. Upon completion of data entry and processing, the paper records are stored in an offsite security storage facility accessible only to

authorized personnel.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are accessed by individual name, social security number, date of birth, and/or by licensee name or number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records managed using REIRS are scheduled under NRC's NUREG-0910, Revision 4. Transfer a copy of REIRS data to the National Archives and Records Administration every 5 years (2.19.16). Retain Personnel monitoring reports and personnel overexposure reports entered into REIRS, Paper records, are retained under 2.19.14.a(1). Destroy 2 years after data are input into REIRS. ADAMS PDFs and TIFFs are retained under 2.19.14.a(4). Cut off electronic files at end of fiscal year. Destroy 2 years after cutoff. Personnel monitoring reports and personnel overexposure reports of which only selected data are entered into REIRS, Paper records, are retained under 2.19.14.b(1). Cut off at end of fiscal year. Transfer to NARA when 20 years old. ADAMS PDFs and TIFFs are retained under 2.19.14.b(4). Cut off electronic files at end of fiscal year. Transfer to the National Archives and Records Administration when 2 years old. Destroy NRC copy 18 years after transferring records.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Information maintained at ORAU is accessible by the Office of Nuclear Regulatory Research (RES) and individuals that have been authorized access by NRC, including all NRC Radiation Safety Officers and ORAU employees that are directly involved in the REIRS project. Reports received and reviewed by the NRC's RES, NRR, NMSS, and Regional offices are in lockable file cabinets and bookcases in secured buildings. A log is maintained of both telephone and written requests for information.

The data maintained in the REIRS database are protected from unauthorized access by several means. The database server resides in a protected environment with physical security barriers under key-card access control. Accounts authorizing access to the server and

databases are maintained by the ORAU REIRS system administrator. In addition, ORAU maintains a computer security “firewall” that further restricts access to the ORAU computer network. Authorization for access must be approved by NRC, ORAU project management, and ORAU computer security. Transmittal of data via the Internet is protected by data encryption.

RECORD ACCESS PROCEDURES:

Same as “Notification procedures.”

CONTESTING RECORD PROCEDURES:

Same as “Notification procedures.”

NOTIFICATION PROCEDURES:

Individuals seeking to determine whether this system of records contains information about them should write to the Freedom of Information Act or Privacy Act Officer, Office of the Chief Information Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, and comply with the procedures contained in NRC’s Privacy Act regulations, 10 CFR part 9.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.