NUCLEAR REGULATORY COMMISSION

[NRC–2019–0191]

Privacy Act of 1974; Systems of Records

AGENCY: Nuclear Regulatory Commission.

ACTION: Notice of modified system of records; request for comments.

SUMMARY: Pursuant to the Privacy Act of 1974 and Office of Management and Budget (OMB) Circular No. A–108, notice is hereby given that the U.S. Nuclear Regulatory Commission (NRC), proposes to modify 28 and rescind 9 of its system of records notices. The proposed modifications would include incorporating, for the convenience of readers, the full text of routine uses previously described in a Prefatory Statement of General Routine Uses directly into each individual system notice to which they apply, incorporating system-breach notification routine uses into each system notice in accordance with OMB Memorandum M–17–12, narrowing the scope of one system notice to eliminate, in accordance with OMB Circular A–108, the partial duplication of a government-wide system of records notice, and eliminating a redundant routine use from one system notice. Of the proposed rescindments of system notices, six would eliminate, in accordance with OMB Circular A–108, notices that duplicate government-wide system of records notices, and three would eliminate notices that are no longer necessary because the records they cover do not qualify as Privacy Act records. Additional details are provided in the **SUPPLEMENTARY INFORMATION** section of this document.

DATES: Submit comments on revisions and changes by January 27, 2020. Comments received after this date will be considered if it is practical to do so, but the Commission is able to ensure consideration only for comments received before this date.

ADDRESSES: You may submit comments by any of the following methods:

- *Federal Rulemaking website:* Go to *https://www.regulations.gov* and search for Docket ID NRC–2019–0191. Address questions about NRC docket IDs in *Regulations.gov* to Jennifer Borges; telephone: 301–287–9127; email: *Jennifer.Borges@nrc.gov.* For technical questions, contact the individual listed in the **FOR FURTHER INFORMATION CONTACT** section of this document.
- *Mail comments to:* Office of Administration, Mail Stop: TWFN–7–A60M, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001, ATTN: Program Management, Announcements and Editing Staff.

For additional direction on obtaining information and submitting comments, see ''Obtaining Information and Submitting Comments'' in the **SUPPLEMENTARY INFORMATION** section of this document.

FOR FURTHER INFORMATION CONTACT: Sally Hardy, Office of the Chief Information Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001, telephone: 301–415–5607; email: *Sally.Hardy@nrc.gov.*

SUPPLEMENTARY INFORMATION

I. Obtaining Information and Submitting Comments

A. Obtaining Information

Please refer to Docket ID NRC–2019–0191 when contacting the NRC about the availability of information for this action. You may obtain publicly-available information related to this action by any of the following methods:

- *Federal Rulemaking website:* Go to *https://www.regulations.gov* and search for Docket ID NRC–2019–0191.
- *NRC's Agencywide Documents Access and Management System (ADAMS):* You may obtain publicly-available documents online in the ADAMS Public Documents collection at *https://www.nrc.gov/reading-rm/adams.html.* To begin the search, select ''*Begin Web-based ADAMS Search.*'' For problems with ADAMS, please contact the NRC's Public Document Room (PDR) reference staff at 1–800–397–4209, 301–415–4737, or by email to *pdr.resource@nrc.gov.*
- *NRC's PDR:* You may examine and purchase copies of public documents at the NRC's PDR, Room O1–F21, One White Flint North, 11555 Rockville Pike, Rockville, Maryland 20852.

B. Submitting Comments

Please include Docket ID NRC–2019–0191 in your comment submission.

The NRC cautions you not to include identifying or contact information that you do not want to be publicly disclosed in your comment submission. The NRC will post all comment submissions at *https://www.regulations.gov* as well as enter the comment submissions into ADAMS. The NRC does not routinely edit comment submissions to remove identifying or contact information.

If you are requesting or aggregating comments from other persons for submission to the NRC, then you should inform those persons not to include identifying or contact information that they do not want to be publicly disclosed in their comment submission. Your request should state that the NRC does not routinely edit comment submissions to remove such information before making the comment submissions available to the public or entering the comment into ADAMS.

II. Background

Pursuant to the Privacy Act of 1974 and OMB Circular No. A–108, ''Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act,'' notice is hereby given that the NRC proposes to modify 28 and rescind 9 of its system of records notices.

First, the NRC is proposing revisions to eliminate its Prefatory Statement of General Routines Uses, in which the NRC has previously listed, as part of its periodic republication of all NRC system notices in the **Federal Register**, those routine uses that are common to many individual system of records notices. Individual system notices have then incorporated any applicable Prefatory Statement routine uses by reference, which has required readers to refer back to the Prefatory Statement earlier in the **Federal Register** notice to understand the full range of routine uses applicable to each system. Under new approach the NRC proposes here, each individual notice would now include the full text of each applicable routine use, including those that were previously included in the Prefatory Statement.

The NRC also proposes to add a new routine use and revise an existing routine use that will apply to all 28 remaining system of records notices, which were most recently published on November 17, 2016 (81 FR 81320), that would authorize the NRC to disclose information when reasonably necessary to respond to a suspected or confirmed breach of an NRC system of records or, as appropriate, to assist another agency in its own response to a suspected or confirmed breach. These changes are in accordance with OMB Memorandum, M–17–12, ''Preparing for and Responding to a Breach of Personally Identifiable Information,'' dated January 3, 2017.

The final proposed change involving routine uses involves removing a routine use addressing disclosures to the Congress from one NRC system notice, because that routine use is redundant in light of 5 U.S.C. 552a(b)(9), which already expressly permits disclosures of Privacy Act information to either House of Congress or to Congressional committees or subcommittees with jurisdiction. The

same system of records notice also has been incorporating a routine use from the Prefatory Statement of General Routine Uses that provides for disclosure of an individual's records to a Member of Congress who is inquiring at the individual's request. The system notice will continue to include that routine use.

In addition, based on a systematic review of its systems of records, the NRC proposes to rescind nine system of records notices. The NRC has determined that six of these notices are duplicative of government-wide systems of records notices. Consistent with guidance in OMB Circular A–108, the NRC proposes to rescind these six duplicative NRC notices. The information these duplicative notices have addressed would still be managed in accordance with the Privacy Act, consistent with the applicable government-wide system of records notices. As to the other three system of records notices the NRC proposes to rescind, the NRC has determined that none of those systems currently involves information about individuals intended for retrieval by agency personnel using the individual's name or other personal identifier. Accordingly, these notices are unnecessary to maintain, as they no longer address Privacy Act systems of records.

The NRC also proposes to narrow the scope of one system of records notice that partially duplicates a government-wide system notice and rename the NRC system to reflect the narrower set of records that the NRC notice will continue to cover. The records no longer addressed by the NRC system notice would still be managed in accordance with the Privacy Act, consistent with the applicable government-wide system of records notice.

The proposed changes to individual NRC system of records notices are as follows:

(1) The NRC proposes to rescind NRC 2, Biographical Information Records, because the information covered by the NRC 2 system notice is all publicly available and intended for informational use by the general public, rather than for retrieval and business use by NRC personnel. The NRC does not currently maintain, or anticipate maintaining, internal, non-publicly available records under this system notice. As such, the records addressed by NRC 2 no longer qualify as a Privacy Act system of records, rendering the system notice for these records unnecessary.

(2) The NRC proposes to remove a Congressional-disclosure routine use in NRC 3, Enforcement Actions Against Individuals. The Privacy Act already expressly permits disclosure of Privacy Act records to either House of Congress and to Congressional committees and subcommittees with jurisdiction, and NRC 3 already includes another routine use addressing disclosure to an individual Member of Congress inquiring on behalf of the individual. Accordingly, the routine use the NRC proposes to remove is unnecessary to retain, because it would allow uses of records that are already permitted by the Privacy Act itself or by another routine use in the same system notice.

(3) The NRC proposes to rescind NRC 4, Conflict of Interest Records, because those records are covered under the government-wide systems OGE/GOVT–1 (Executive Branch Personnel Public Financial Disclosure Reports and Other Name-Retrieved Ethics Program Records) and OGE/GOVT–2 (Executive Branch Confidential Financial Disclosure Reports). Rescinding NRC 4 would avoid duplicative notices.

(4) The NRC proposes to rescind NRC 6, Department of Labor (DOL) Discrimination Cases, because these records are no longer retrieved by name or personal identifier.

(5) The NRC proposes to rescind NRC 9, Office of SBCR Discrimination Complaint Records, because those records are covered under the government-wide system EEOC/GOVT–1 (Equal Employment Opportunity in the Federal Government Complaint and Appeal Records). Rescinding NRC 9 would avoid duplicative notices.

(6) The NRC proposes to modify NRC 11, General Personnel Records (Official Personnel Folder and Related Records). NRC 11 is a partial duplicate of the government-wide system OPM/GOVT–1 (General Personal Records). The modification would narrow the scope of NRC 11 so that the system includes only those records that OPM/GOVT–1 does not also include: Specifically, reasonable accommodation records. This modification would therefore ensure that the NRC 11 notice does not duplicate the government-wide OPM/GOVT–1 notice. In connection with this modification, the NRC also proposes to rename NRC 11 to ''Reasonable Accommodations Records—NRC'' to better describe the records that would remain in the system.

(7) The NRC proposes to rescind NRC 17, Occupational Injury and Illness Records, because those records are covered under the government-wide system DOL/GOVT–1 (Office of Worker's Compensation Programs, Federal Employees' Compensation Act File). Rescinding NRC 17 would avoid duplicative notices.

(8) The NRC proposes to rescind NRC 20, Official Travel Records, because those records are covered under the government-wide system GSA/GOVT–4 (Contracted Travel Services Program). Rescinding NRC 20 would avoid duplicative notices.

(9) The NRC proposes to rescind NRC 22, Personnel Performance Appraisals, because those records are covered under the government-wide system OPM/GOVT–2 (Employee Performance File System Records). Rescinding NRC 22 would avoid duplicative notices.

(10) The NRC proposes to rescind NRC 28, Merit Selection Records, because those records are covered under the government-wide system OPM/GOVT–5 (Recruiting, Examining, and Placement Records). Rescinding NRC 28 would avoid duplicative notices.

(11) The NRC proposes to rescind NRC 42, Strategic Workforce Planning Records. Because of the purpose and functionality of the new database the NRC is using to manage the records involved, the records are no longer retrieved by name or personal identifier.

(12) The NRC proposes to update all remaining NRC system notices (that is, the system notices the NRC would not be rescinding) to include the full text of any applicable routine uses that previously have been contained in the Prefatory Statement of General Routine Uses. These revisions are not intended to modify the routine uses applicable to these systems. The purpose is solely for the convenience of the reader: To eliminate the need, when reviewing a particular system notice in the **Federal Register**, to refer back to a Prefatory Statement earlier in the **Federal Register** notice.

(13) The NRC proposes to update all remaining NRC system notices (that is, the system notices the NRC would not be rescinding) to include the routine use language associated with responding to system breaches in accordance with OMB Memorandum M–17–12.

The proposed revisions and rescindments to these systems require an advance period for public comment.

A report on these revisions and rescindments has been sent to OMB, the Committee on Homeland Security and Governmental Affairs of U.S. Senate, and the Committee on Oversight and Reform of the U.S. House of Representatives, as required by the Privacy Act.

If changes are made based on the NRC's review of comments received, the NRC will publish a subsequent notice.

The text of the report, in its entirety, is attached.

Dated at Rockville, Maryland, this 17th day of December, 2019.

For the Nuclear Regulatory Commission.

Scott C. Flanders,

Senior Agency Official for Privacy,

Office of the Chief Information Officer.

Attachment—Nuclear Regulatory Commission Privacy Act Systems of Records

NRC SYSTEMS OF RECORDS

1. Parking Permit Records—NRC.
2. (Rescinded.)
3. Enforcement Actions Against Individuals—NRC.
4. (Rescinded.)
5. Contracts Records—NRC.
6. (Rescinded.)
7. (Rescinded.)
8. Employee Disciplinary Actions, Appeals, Grievances, and Complaints Records—NRC.
9. (Rescinded.)
10. Freedom of Information Act (FOIA) and Privacy Act (PA) Request Records—NRC.
11. Reasonable Accommodations Records—NRC.
12. Child Care Subsidy Program Records—NRC.
13. (Rescinded.)
14. Employee Assistance Program Records—NRC.
15. (Rescinded.)
16. Facility Operator Licensees Records (10 CFR part 55)—NRC.
17. (Rescinded.)
18. Office of the Inspector General (OIG) Investigative Records—NRC and Defense Nuclear Facilities Safety Board (DNFSB).
19. Official Personnel Training Records—NRC.
20. (Rescinded.)
21. Payroll Accounting Records—NRC.
22. (Rescinded.)
23. Office of Investigations Indices, Files, and Associated Records—NRC.
24. (Rescinded.)
25. Oral History Program—NRC.
26. Transit Subsidy Benefits Program Records—NRC.
27. Radiation Exposure Information and Reporting System (REIRS) Records—NRC.
28. (Rescinded.)
29. (Rescinded.)
30. (Rescinded.)
31. (Rescinded.)
32. Office of the Chief Financial Officer Financial Transactions and Debt Collection Management Records—NRC.
33. Special Inquiry Records—NRC.
34. (Rescinded.)
35. Drug Testing Program Records—NRC.
36. Employee Locator Records—NRC.
37. Information Security Files and Associated Records—NRC.
38. Mailing Lists—NRC.
39. Personnel Security Files and Associated Records—NRC.
40. Facility Security Access Control Records—NRC.
41. Tort Claims and Personal Property Claims Records—NRC.
42. (Rescinded.)
43. Employee Health Center Records—NRC.
44. Employee Fitness Center Records—NRC.
45. Electronic Credentials for Personal Identity Verification—NRC.

These systems of records are those systems maintained by the NRC that contain personal information about individuals from which information is retrieved by an individual's name or identifier.

The notice for each system of records states the name and location of the record system, the authority for and manner of its operation, the categories of individuals that it covers, the types of records that it contains, the sources of information in those records, and the routine uses of each system of records. Each notice also includes the business address of the NRC official who will inform interested persons of the procedures whereby they may gain access to and request amendment of records pertaining to them.

The Privacy Act provides certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies to protect records contained in an agency system of records from unauthorized disclosure and to ensure that information is current and accurate for its intended use and that adequate safeguards are provided to prevent misuse of such information.

SYSTEM NAME AND NUMBER:

Parking Permit Records—NRC 1.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Facility Operations and Space Management Branch, Office of Administration, NRC, Two White Flint North, 11555 Rockville Pike, Rockville, Maryland, and current contractor facility.

SYSTEM MANAGER(S):

Chief, Facility Operations and Space Management Branch, Division of Facilities and Security, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

31 U.S.C. 3511; 41 CFR 102–74.265 *et seq.,* Parking Facilities.

PURPOSE(S) OF THE SYSTEM:

The information contained in this system is used for the assignment of parking permits and NRC-controlled parking spaces.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

NRC employees and contractors who apply for parking permits for NRC-controlled parking spaces.

CATEGORIES OF RECORDS IN THE SYSTEM:

These records consist of the applications and the revenue collected for the Headquarters' parking facilities. The applications include, but are not limited to, the applicant's name, address, telephone number, length of service, vehicle, rideshare, and handicap information.

RECORD SOURCE CATEGORIES:

Applications submitted by NRC employees and contractors.

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 record amount paid and revenue collected for parking;

b. To contact permit holder;

c. To determine priority for issuance of permits;

d. To provide statistical reports to city, county, State, and Federal Government agencies;

e. 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;

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 in file folders and on electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Accessed by name, tag number, and/or permit number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained under the National Archives and Records Administration's General Records Schedule 5.6: Security Records, Item 130, Local facility identification and card access records. Records are destroyed upon immediate collection once the temporary credential or card is returned for potential reissuance due to nearing expiration or not to exceed 6 months from time of issuance or when individual no longer requires access, whichever is sooner, but longer retention is authorized if required for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Paper records are maintained in locked file cabinets under visual control of the Facility Operations and Space Management Branch staff. Computer files are maintained on a hard drive, access to which is password protected. Access to and use of these records is limited to those persons whose official duties require access.

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.

NRC–2 (Rescinded.)

RESCINDMENT OF SYSTEM OF RECORDS NOTICE:

SYSTEM NAME AND NUMBER:

Biographical Information Records—NRC 2.

SYSTEM MANAGER:

Senior Advisor, Office of Public Affairs, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

HISTORY:

These notices were last published in the **Federal Register** on November 17, 2016 (81 FR 81320).

SYSTEM NAME AND NUMBER:

Enforcement Actions Against Individuals—NRC 3.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Primary system—Office of Enforcement, NRC, One White Flint North, 11555 Rockville Pike, Rockville, Maryland.

Duplicate system—Duplicate systems may exist, in whole or in part, at the NRC Regional Offices at the locations listed in Addendum I, Part 2, and in the Office of the General Counsel, NRC, One White Flint North, 11555 Rockville Pike, Rockville, Maryland.

SYSTEM MANAGER(S):

Director, Office of Enforcement, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

42 U.S.C. 2073(e), 2113, 2114, 2167, 2168, 2201(i), 2231, 2282; 10 CFR 30.10, 40.10, 50.5, 50.110, 50.111, 50.120, 60.11, 61.9b, 70.10, 72.12, 110.7b, 110.50, and 110.53; 10 CFR part 2, subpart B; Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 *et seq.*); 10 CFR 19.16(a), 30.7, 40.7, 50.7, 60.9, 70.7, and 72.10; Energy Reorganization Act of 1974, as amended, section 211 (42 U.S.C. 5851); 5 U.S.C. 2302(a)(2)(A).

PURPOSE(S) OF THE SYSTEM:

The purpose of the system is to maintain information about individuals involved in NRC-licensed activities who have been subject to NRC enforcement actions or who have been the subject of correspondence indicating that they are being or have been considered for enforcement action.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals involved in NRC-licensed activities who have been subject to NRC enforcement actions or who have been the subject of correspondence indicating that they are being, or have been, considered for enforcement action.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system includes, but is not limited to, individual enforcement actions, including Orders, Notices of Violations with and without Civil Penalties, Orders Imposing Civil Penalties, Letters of Reprimand, Demands for Information, and letters to individuals who are being or have been considered for enforcement action. Also included are responses to these actions and letters. In addition, the files may contain other relevant documents directly related to those actions and letters that have been issued. Files are arranged numerically by Individual Action (IA) numbers, which are assigned when individual enforcement actions are considered. In instances where only letters are issued, these

letters also receive IA numbers. The system includes a computerized database from which information is retrieved by names of the individuals subject to the action and IA numbers.

RECORD SOURCE CATEGORIES:

Information in the records is primarily obtained from NRC inspectors and investigators and other NRC employees, individuals to whom a record pertains, authorized representatives for these individuals, and NRC licensees, vendors, other individuals regulated by the NRC, and persons making allegations to the NRC.

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 deter future violations, certain information in this system of records may be routinely disseminated to the public by means such as publishing in the **Federal Register** certain enforcement actions issued to individuals and making the information available in the Public Document Room accessible through the NRC website, *www.nrc.gov;*

b. When considered appropriate for disciplinary purposes, information in this system of records, such as enforcement actions and hearing proceedings, may be disclosed to a bar association, or other professional organization performing similar functions, including certification of individuals licensed by NRC or Agreement States to perform specified licensing activities;

c. Where appropriate to ensure the public health and safety, information in this system of records, such as enforcement actions and hearing proceedings, may be disclosed to a Federal or State agency with licensing jurisdiction;

d. To respond to the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. 2904 and 2906;

e. 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;

f. 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;

g. 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;

h. 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;

i. 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;

j. 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;

k. 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

l. 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 in file folders and on computer media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are accessed by individual action file number or by the name of the individual.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Cut off files when case is closed. Hold 5 years and retire to Washington National Records Center (WNRC). Transfer to NARA with related indexes when 20 years old. (NUREG–0910, Rev. 4, 2.10.2.a(1)). Cut off electronic files when case is closed. Transfer to NARA 2 years after cutoff. Destroy NRC copy 18 years after transferring record to NARA (NUREG–0910, Rev. 4, 2.10.2.a(4)).

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Paper records are maintained in lockable file cabinets and are under visual control during duty hours. Access to computer records requires use of proper password and user identification codes. Access to and use of these records is limited to those NRC employees whose official duties require access.

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.

NRC–4 (Rescinded.)

RESCINDMENT OF SYSTEM OF RECORDS NOTICE:

SYSTEM NAME AND NUMBER:

Conflict of Interest Records—NRC 4.

SYSTEM MANAGER:

Assistant General Counsel for Legal Counsel, Legislation, and Special Projects, Office of the General Counsel, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

HISTORY:

These notices were last published in the **Federal Register** on November 17, 2016 (81 FR 81320).

SYSTEM NAME AND NUMBER:

Contracts Records—NRC 5.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Primary system—Acquisition Management Division, Office of Administration, NRC, Two White Flint North, Rockville, Maryland.

Duplicate system—Duplicate systems exist, in part, at the locations listed in Addendum I, Parts 1 and 2, in working files maintained by the assigned contracting office representative and in the NRC's Agencywide Documents Access and Management System (ADAMS).

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

15 U.S.C. 631, 644; 31 U.S.C. 3511; 13 CFR 124.501–520; 44 U.S.C. 3301; 48 CFR subpart 4.8; 48 CFR part 19.

PURPOSE(S) OF THE SYSTEM:

This system consists of contract file documentation as required by the Federal Acquisition Regulation (FAR) Subpart 4.8—Government Contract Files. The automated system assists with the generation of and maintenance of the file documentation.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Persons who are employed as NRC contractors. NRC employees substantially involved with contracting, such as contracting office representatives and other acquisition officials.

CATEGORIES OF RECORDS IN THE SYSTEM:

These records contain personal information (such as technical qualifications, education, rates of pay, employment history) of contractors and their employees, and other contracting records. They also contain evaluations, recommendations, and reports of NRC acquisition officials, assessment of contractor performance, invoice payment records, and related information.

RECORD SOURCE CATEGORIES:

Information in this system of records comes from the contractor or potential contractor or NRC employee.

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 information to the Federal Procurement Data System—Next Generation, U.S. Department of Health and Human Services, U.S. Defense Contract Audit Agency, U.S. Government Accountability Office, and other Federal agencies for audits and reviews;

b. 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;

c. 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;

d. 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;

e. 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;

f. 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;

g. 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;

h. 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

i. 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 in file folders and on computer media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Paper records are accessed by contract number or purchase order number; and are cross-referenced to the automated system that contains the name of the contractor, vendor, contracting office representative, contracting officer, and taxpayer identification number (TIN).

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained under the National Archives and Records Administration's General Records Schedule 1.1: Financial Management and Reporting Records, Item 010, Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting, as the official record held in the office of record. Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use. Records are also retained under General Records Schedule 1.1: Financial Management and Reporting Records, Item 011, Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting, all other copies. Destroy when business use ceases.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

File folders are maintained in unlocked conserver files in a key code locked room. Access to and use of these records is limited to those persons whose official duties require such access. Select individuals have access through use of their badges. Access to automated systems is protected by passwords and roles and responsibilities.

SYSTEM MANAGER(S):

Director, Acquisition Management Division, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

RECORD ACCESS PROCEDURES:

Same as ''Notification procedures.'' Some information was received in confidence and will not be disclosed to the extent that disclosure would reveal confidential business (proprietary) information.

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:

Pursuant to 5 U.S.C. 552a(k)(1) and (k)(5), the Commission has exempted portions of this system of records from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f).

NRC–6 (Rescinded.)

RESCINDMENT OF SYSTEM OF RECORDS NOTICE:

SYSTEM NAME AND NUMBER:

Department of Labor (DOL) Discrimination Cases—NRC 6.

SYSTEM MANAGER:

Director, Office of Enforcement, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

HISTORY:

These notices were last published in the **Federal Register** on November 17, 2016 (81 FR 81320).

NRC–7 (Rescinded.)

SYSTEM NAME AND NUMBER:

Employee Disciplinary Actions, Appeals, Grievances, and Complaints Records—NRC 8.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Primary system—Office of the Chief Human Capital Officer, NRC, Two White Flint North, 11545 Rockville Pike, Rockville, Maryland.

The Office of the Inspector General (OIG) employee files are located with the NRC's OIG, 11555 Rockville Pike, Rockville, Maryland.

Duplicate system—A duplicate system may be maintained, in whole or in part, in the Office of the General Counsel, NRC, One White Flint North, 1555 Rockville Pike, Rockville, Maryland, and at NRC's Regional Offices at locations listed in Addendum I, Part 2.

SYSTEM MANAGER(S):

Chief, Policy, Labor and Employee Relations Branch, Office of the Chief Human Capital Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001. For OIG employee records: Director, Resource Management and Operations Support, Office of the Inspector General, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 3132(a); 5 U.S.C. 3521–3525; 5 U.S.C. 4303, as amended; 5 U.S.C. 7503; 29 U.S.C. 633a; 29 U.S.C. 791; 42 U.S.C. 2000e–16; 42 U.S.C. 2201(d), as amended.

PURPOSE(S) OF THE SYSTEM:

The purpose of this system is to document all current and former NRC employees and annuitants who have filed complaints, grievances or appeals or the subject of proposed or final disciplinary action or have been suspected of misconduct.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Current and former NRC employees, and annuitants who have filed written complaints brought to the Office of the Chief Human Capital Officer's attention or initiated grievances or appeal proceedings as a result of a determination made by the NRC, Office of Personnel Management, and/or Merit Systems Protection Board, or a Board or other entity established to adjudicate such grievances and appeals.

CATEGORIES OF RECORDS IN THE SYSTEM:

Includes all documents related to: Disciplinary actions; adverse actions; appeals; complaints, including but not limited to those raised under the agency's prevention of harassment program; grievances; arbitrations; and negative determinations regarding within-grade salary increases. It contains information relating to determinations affecting individuals made by the NRC, Office of Personnel Management, Merit Systems Protection Board, arbitrators or courts of law. The records may include the initial appeal or complaint, letters or notices to the individual, records of hearings when conducted, materials placed into the record to support the decision or determination, affidavits or statements, testimony of witnesses, investigative reports, instructions to an NRC office or division concerning action to be taken to comply with decisions, and related correspondence, opinions, and recommendations.

RECORD SOURCE CATEGORIES:

Individuals to whom the record pertains, NRC, Office of Personnel Management and/or Merit Systems Protection Board officials; affidavits or statements from employees, union representatives, or other persons; testimony of witnesses; official documents relating to the appeal, grievance, or complaint, including but not limited to those raised under the agency's prevention of harassment

program; Official Personnel Folder; and other Federal agencies.

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 furnish information to the Office of Personnel Management and/or Merit Systems Protection Board under applicable requirements related to grievances and appeals;

b. To provide appropriate data to union representatives and third parties (that may include the Federal Services Impasses Panel and Federal Labor Relations Authority) in connection with grievances, arbitration actions, and appeals;

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 computer media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are retrieved by individual's name.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained under the National Archives and Records Administration's General Records Schedule 2.3: Employee Relations Records, Administrative grievance, disciplinary, and adverse action files, Item 060, Administrative grievance files, Item 061, Adverse action files, and Item 062, Performance-based action files, respectively. Destroy no sooner than 4 years but no less than 7 years after case is closed.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records are maintained in locked file cabinets and in a password-protected automated system. Access to and use of these records is limited to those persons whose official duties require such access.

RECORD ACCESS PROCEDURES:

Same as ''Notification procedures.'' Some information was received in confidence and will not be disclosed to the extent that disclosure would reveal a confidential source.

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.

NRC–9 (Rescinded.)

RESCINDMENT OF SYSTEM OF RECORDS NOTICE:

SYSTEM NAME AND NUMBER:

Office of SBCR Discrimination Complaint Records—NRC 9.

SYSTEM MANAGER:

Associate Director, Civil Rights and Diversity Directorate and Associate Director, Small Business, Outreach and Compliance Directorate, Office of Small Business and Civil Rights, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

HISTORY:

These notices were last published in the **Federal Register** on November 17, 2016 (81 FR 81320).

SYSTEM NAME AND NUMBER:

Freedom of Information Act (FOIA) and Privacy Act (PA) Request Records—NRC 10.

SECURITY CLASSIFICATION:

Classified and Unclassified.

SYSTEM LOCATION:

Primary system—FOIA, Privacy, Info Collections Branch, Customer Service Division, Office of the Chief Information Officer, NRC, Two White Flint North, 11545 Rockville Pike, Rockville, Maryland.

Duplicate system—Duplicate systems may exist, in part, at the locations listed in Addendum I, Parts 1 and 2.

SYSTEM MANAGER(S):

FOIA Officer, Information Services Branch, Governance & Enterprise Management Services Division, Office of the Chief Information Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 552 and 552a; 42 U.S.C. 2201, as amended; 10 CFR part 9.

PURPOSE(S) OF THE SYSTEM:

The purpose of this system is to support the processing of record access requests and administrative appeals under the FOIA, as well as access, notification, and amendment requests and administrative appeals under the Privacy Act, whether NRC receives such requests directly from the requester or via referral from another agency. In addition, this system is used to support agency participation in litigation arising from such requests and appeals, and to assist NRC in carrying out any other responsibilities under the FOIA or the access or amendment provisions of the Privacy Act.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals filing requests for access to information under the Freedom of Information Act (FOIA) or Privacy Act (PA); individual's names in the FOIA request; NRC staff assigned to help process, consider, and respond to such requests, including any appeals.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system contains copies of the written requests from individuals or organizations made under the FOIA or PA, the NRC response letters, and related records.

RECORD SOURCE CATEGORIES:

Requests are made by individuals. The response to the request is based upon information contained in NRC records.

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. If an appeal or court suit is filed with respect to any records denied;

b. For preparation of reports required by 5 U.S.C. 552 and 5 U.S.C. 552a;

c. To another Federal agency when consultation or referral is required to process a request;

d. 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;

e. 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;

f. 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;

g. 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;

h. 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;

i. 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;

j. 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;

k. A record from this system of records may be disclosed as a routine use to respond to the National Archives and Records Administration, Office of Government Information Services (OGIS), to the extent necessary to allow OGIS to fulfill its responsibilities under 5 U.S.C. 552(h), to review administrative agency policies, procedures and compliance with the Freedom of Information Act (FOIA) and offer mediation services to resolve disputes between persons making FOIA requests and administrative agencies; and

l. 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.

m. FOIA records, which are publicly available in the Public Documents Room, are accessible through the NRC website, *http://www.nrc.gov.*

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are maintained on paper, audio and video tapes, and electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are accessed by unique assigned number for each request and by requester's name.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained under the National Archives and Records Administration's, General Records Schedule 4.2: Information Access and Protection Records, Item 020, Access and disclosure request files. Destroy 6 years after final agency action or 3 years after final adjudication by the courts, whichever is later, but longer retention is authorized if required for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records are maintained in locked file cabinets that are kept in locked rooms. Electronic records are password protected. Access to and use of these records is limited to those persons whose official duties require such access.

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:

Records contained in this system that have been placed on the NRC public website are available upon request. Pursuant to 5 U.S.C. 552a(k)(2), records in this system, which reflect records that are contained in other systems of records that are designated as exempt, are exempt from the requirements of subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), (I), and (f) of 5 U.S.C. 552a.

SYSTEM NAME AND NUMBER:

Reasonable Accommodation Records—NRC 11.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Primary system—For Headquarters and all Senior Executive Service (SES) personnel, Office of the Chief Human Capital Officer, NRC, Two White Flint North, 11545 Rockville Pike, Rockville, Maryland. For Regional personnel, at Regional Offices I–IV listed in Addendum I, part 2.

SYSTEM MANAGER(S):

Associate Director for Human Resources Operations and Policy, Office of the Chief Human Capital Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Executive Order (E.O.) 13164, as amended by E.O. 13478.

PURPOSE(S) OF THE SYSTEM:

To allow the NRC to collect and maintain records on applicants for employment as well as employees with disabilities who requested or received reasonable accommodation by the Department as required by Sections 501, 504, and 701 of the Rehabilitation Act of 1973.This system will track and report the processing of requests for reasonable accommodation to comply with applicable law and regulations and to preserve and maintain confidentiality.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Federal employees requesting a reasonable accommodation.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system name, accommodation being requested, accommodation type, impairment, disability type, disability condition, 504/508 explanation, and case notes.

RECORD SOURCE CATEGORIES:

Information in this system of records comes from the individual to whom it applies; is derived from information supplied by that individual; employee's supervisor or private and Federal physicians, and medical institutions.

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. A record from this system of records may be disclosed as a routine use to a prospective employer of a Government employee. Upon transfer of the employee to another Federal agency, the information is transferred to such agency;

b. A record from this system of records may be disclosed as a routine use to provide information to the OPM and/or MSPB for review, audit, or reporting purposes;

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 in file folders and on electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are retrieved by employee name.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained under the National Archives and Records Administration's General Records Schedule 2.3: Employee Relations Records, Item 020, Reasonable accommodation records, Reasonable accommodation program files, and Item 021, Reasonable accommodation employee case files. Destroy 3 years after being superseded, but longer retention is authorized if required for business use (Item 020). Destroy 3 years after employee separation from the agency or all appeals are concluded, whichever is later, but longer retention is authorized if required for business use (Item 021).

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records are maintained on paper and electronically. Paper documents are maintained in lockable file cabinets. Electronic files are password protected.

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.

SYSTEM NAME AND NUMBER:

Child Care Subsidy Program Records—NRC 12.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

DecisionPoint Corporation, 702 Russell Ave., Suite 312, Gaithersburg, MD 20877.

SYSTEM MANAGER(S):

Associate Director for Human Resources Operations and Policy, Office of the Chief Human Capital Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

40 U.S.C. 590(g); 5 CFR 792.201–206; Executive Order (E.O.) 9397, as amended by E.O. 13478.

PURPOSE(S) OF THE SYSTEM:

The purpose of this system is to administer NRC-sponsored childcare program.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

NRC employees who voluntarily apply for child care subsidy.

CATEGORIES OF RECORDS IN THE SYSTEM:

These records include application forms for child care subsidy containing personal information about the employee (parent), their spouse (if applicable), their child/children, and their child care provider, including name, social security number, employer, grade, home and work telephone numbers, home and work addresses, total family income, name of child on whose behalf the parent is applying for subsidy, child's date of birth; information on child care providers used, including name, address, provider license number and State where issued, child care cost, and provider tax identification number; and copies of IRS Form 1040 or 1040A for verification purposes.

RECORD SOURCE CATEGORIES:

Information is obtained from NRC employees who apply for child care subsidy and their child care provider.

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. A record from this system of records may be disclosed as a routine use to the Office of Personnel Management to provide statistical reports;

b. 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;

c. 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;

d. 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;

e. 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;

f. 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;

g. 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;

h. 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

i. 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 at the current contractor site.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Information may be retrieved by employee name or social security number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained under the National Archives and Records Administration's General Records Schedule 2.4: Employee Compensation and Benefits Records, Item 120, Child care subsidy program administrative records. Destroy when 3 years old, but longer retention is authorized if required for business use. Child care subsidy program individual case files are retained under General Records Schedule 2.4, Item 121. Destroy 2 years after employee participation concludes, but longer retention is authorized if required for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

When not in use by an authorized person, paper records are stored in lockable file cabinets and computer records are protected by the use of passwords.

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.

NRC–13 (Rescinded.)

SYSTEM NAME AND NUMBER:

Employee Assistance Program Records—NRC 14.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Office of the Chief Human Capital Officer, NRC, Two White Flint North, 11545 Rockville Pike, Rockville, Maryland, and current contractor facility.

RECORD SOURCE CATEGORIES:

Information compiled by the Employee Assistance Program Manager, and the Employee Assistance Program contractor during the course of counseling with an NRC employee or members of the employee's family.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 7901; 21 U.S.C. 1101–1181; 42 U.S.C. chapter 6A, Subchapter III–A; 44 U.S.C. 3101; 44 U.S.C. 3301; 5 CFR 792.101–105.

PURPOSE(S) OF THE SYSTEM:

This record system will maintain information gathered by and in the possession of the NRC EAP, an internal agency program designed to assist employees of NRC and, in certain instances, their families, in regard to a variety of personal and/or work-related issues.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

NRC employees or family members who have been counseled by or referred to the Employee Assistance Program (EAP) for problems relating to alcoholism, drug abuse, job stress, chronic illness, family or relationship concerns, and emotional and other similar issues.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system contains records of NRC employees or their families who have participated in the EAP and the results of any counseling or referrals which may have taken place. The records may contain information as to the nature of each individual's problem, subsequent treatment, and progress.

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: (*Note:* Any disclosure of information pertaining to an individual will be made in compliance with the Confidentiality of Alcohol and Drug Abuse Patient Records regulations, 42 CFR part 2, as authorized by 42 U.S.C. 290dd–2, as amended.)

a. For statistical reporting purposes;

b. 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

c. 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 in file folders and on electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Information accessed by the EAP identification number and name of the individual.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained under the National Archives and Records Administration's General Records Schedule 2.7: Employee Health and Safety Records, Employee Assistance Program (EAP) counseling records, Item 091, Records not related to performance or conduct. Destroy 7 years after termination of counseling for adults or 3 years after a minor reaches the age of majority, or when the state-specific statute of limitations has expired for contract providers subject to state requirements, but longer retention is authorized if needed for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Files are maintained in a safe under the immediate control of the Employee Assistance Program Manager and the current EAP contractor. Case files are maintained in accordance with the confidentiality requirements of Public Law 93–282, any NRC-specific confidentiality regulations, and the Privacy Act of 1974.

SYSTEM MANAGER(S):

Employee Assistance Program Manager, Office of the Chief Human Capital Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

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.

NRC–15 (Rescinded.)

SYSTEM NAME AND NUMBER:

Facility Operator Licensees Records (10 CFR part 55)—NRC 16.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

For power reactors, at the appropriate Regional Office at the address listed in Addendum I, Part 2; for non-power (test and research) reactor facilities, at the Operator Licensing Branch, Division of Inspection and Regional Support, Office of Nuclear Reactor Regulation, NRC, One White Flint North, 11555 Rockville Pike, Rockville, Maryland. The Reactor Program System—Operator Licensing (RPS–OL) is located at NRC Headquarters and is accessible by the four Regional Offices.

SYSTEM MANAGER(S):

Chief, Operator Licensing Branch, Division of Inspection and Regional Support, Office of Nuclear Reactor Regulation, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

42 U.S.C. 2131–2141; 10 CFR part 55.

PURPOSE(S) OF THE SYSTEM:

The purpose of the system is to record information associated with individual operator licenses; including initial applications, examination results, license issuance, license renewals, license expirations, and medical status.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals licensed under 10 CFR part 55, new applicants whose applications are being processed, and individuals whose licenses have expired.

CATEGORIES OF RECORDS IN THE SYSTEM:

These records contain information pertaining to 10 CFR part 55 applicants for a license, licensed operators, and individuals who previously held licenses. This includes applications for a license, license and denial letters, and related correspondence; correspondence relating to actions taken against a licensee; 10 CFR 50.74 notifications; certification of medical examination and related medical information; fitness for duty information; examination results and other docket information.

RECORD SOURCE CATEGORIES:

Information in this system comes from the individual applying for a license, the 10 CFR part 50 licensee, a licensed physician, and NRC and contractor staff.

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 determine if the individual meets the requirements of 10 CFR part 55 to take an examination or to be issued an operator's license;

b. To provide researchers with information for reports and statistical evaluations related to selection, training, and examination of facility operators;

c. To provide examination, testing material, and results to facility management;

d. 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;

e. 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;

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 in file folders and logs, and on electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are accessed by name and docket number and ADAMS accession number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained under the Nuclear Regulatory Commission's (NRC) NUREG 0910 Rev 4—(2.18.6.a, 2.25.9.a), Headquarters and Regional Operator Licensing Files, 10 CFR part 55 Docket Files. Cutoff files upon latest license expiration/revocation/termination, application denial or withdrawal, or issuance of denial letter. Destroy when 10 years old. Examination Package records are retained under NUREG 0910 Rev 4—(2.18.6.b(1), 2.18.6.b(4), 2.25.9.b(1), 2.25.9.b(4)). Cutoff upon receipt of next exam. Destroy 4 years after cutoff.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Maintained in locked file cabinets or an area that is locked. Computer files are password protected. Access to and use of these records is limited to those persons whose official duties require such access based on roles and responsibilities.

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.

NRC–17 (Rescinded.)

RESCINDMENT OF SYSTEM OF RECORDS NOTICE:

SYSTEM NAME AND NUMBER:

Occupational Injury and Illness Records—NRC 17.

SYSTEM MANAGER:

For Headquarters Part 1—Benefits Officer, Human Resources Operations and Policy, Office of the Chief Human Capital Officer, and Part 2—Safety and Occupational Health Manager, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001. For Region I–IV—The appropriate Human Resources Team Leader at the locations listed in Addendum I, Part 2.

HISTORY:

These notices were last published in the **Federal Register** on November 17, 2016 (81 FR 81320).

SYSTEM NAME AND NUMBER:

Office of the Inspector General (OIG) Investigative Records—NRC and Defense Nuclear Facilities Safety Board (DNFSB)—NRC 18.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Office of the Inspector General, NRC, One White Flint North, 11555 Rockville Pike, Rockville, Maryland.

SYSTEM MANAGER(S):

Assistant Inspector General for Investigations, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Inspector General Act of 1978, as amended, 5 U.S.C. app. 3; and the Consolidated Appropriations Act, 2014.

PURPOSE(S) OF THE SYSTEM:

NRC OIG uses records and information collected and maintained in this system to receive and adjudicate allegations/complaints of violations of criminal, civil, and administrative laws and regulations relating to NRC programs, operations, and employees, as well as contractors and other individuals and entities associated with NRC; monitor complaint and investigation assignments, status, disposition, and results; manage investigations and information provided during the course of such investigations; track and assess actions taken by NRC management regarding employee misconduct and other allegations; support and assess legal actions taken following referrals for criminal prosecution or litigation; provide information relating to any adverse action or other proceeding that may occur as a result of the findings of an investigation.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals and entities referred to in complaints or actual investigative cases, reports, accompanying documents, and correspondence prepared by, compiled by, or referred to the OIG.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system comprises five parts: (1) An automated Investigative Database Program containing reports of investigations, inquiries, and other reports closed since 1989; (2) paper files of all OIG and predecessor Office of Inspector and Auditor (OIA) reports, correspondence, cases, matters, memoranda, materials, legal papers, evidence, exhibits, data, and work papers pertaining to all closed and pending investigations, inquiries, and other reports; (3) paper index card files of OIG and OIA cases closed from 1970 through 1989; (4) an automated Investigative Management System that

includes allegations referred to the OIG from 1985 forward, whether or not the allegation progressed to an investigation, inquiry or other report, and dates that an investigation, inquiry or other report was opened and closed and reports, correspondence, cases, matters, memoranda, materials, legal papers, evidence, exhibits, data and work papers pertaining to these cases.

RECORD SOURCE CATEGORIES:

The information is obtained from sources including, but not limited to, the individual record subject; NRC officials and employees; employees of Federal, State, local, and foreign agencies; and other persons.

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, OIG 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 any Federal, State, local, tribal, or foreign agency, or other public authority responsible for enforcing, investigating, or prosecuting violations of administrative, civil, or criminal law or regulation if that information is relevant to any enforcement, regulatory, investigative, or prosecutorial responsibility of the receiving entity when records from this system of records, either by themselves or in combination with any other information, indicate a violation or potential violation of law, whether administrative, civil, criminal, or regulatory in nature;

b. To public or private sources to the extent necessary to obtain information from those sources relevant to an OIG investigation, audit, inspection, or other inquiry;

c. To a court, adjudicative body before which NRC or DNFSB is authorized to appear, Federal agency, individual or entity designated by NRC or DNFSB or otherwise empowered to resolve disputes, counsel or other representative, or witness or potential witness when it is relevant and necessary to the litigation if any of the parties listed below is involved in the litigation or has an interest in the litigation:

1. NRC or DNFSB, or any component of NRC or DNFSB;

2. Any employee of NRC or DNFSB where the NRC or DNFSB or the Department of Justice has agreed to represent the employee; or

3. The United States, where NRC or DNFSB determines that the litigation is likely to affect the NRC or DNFSB or any of their components;

d. To a private firm or other entity with which OIG or NRC or DNFSB contemplates it will contract or has contracted for the purpose of performing any functions or analyses that facilitate or are relevant to an investigation, audit, inspection, inquiry, or other activity related to this system of records, to include to contractors or entities who have a need for such information or records to resolve or support payment to the agency. The contractor, private firm, or entity needing access to the records to perform the activity shall maintain Privacy Act safeguards with respect to information. A contractor, private firm, or entity operating a system of records under 5 U.S.C. 552a(m) shall comply with the Privacy Act;

e. To another agency to the extent necessary for obtaining its advice on any matter relevant to an OIG investigation, audit, inspection, or other inquiry related to the responsibilities of the OIG;

f. To the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. 2904 and 2906;

g. 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;

h. 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;

i. 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;

j. 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;

k. 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;

l. 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;

m. 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

n. 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:

Information is maintained on index cards, in paper files, and on electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Information is retrieved from the Investigative Database Program by the

name of an individual, by case number, or by subject matter. Information in the paper files backing up the Investigative Database Program and older cases closed by 1989 is retrieved by subject matter and/or case number, not by individual identifier. Information is retrieved from index card files for cases closed before 1989 by the name or numerical identifier of the individual or entity under investigation or by subject matter. Information in both the Allegations Tracking System and the Investigative Management System is retrieved by allegation number, case number, or name.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained according to the National Archives and Records Administration's approved schedule for the Office of the Inspector General, N1–431–10–002, item 2.b, Investigation Case Files. Cut off at close of fiscal year in which the case is closed. Transfer to the Federal Records Center (FRC) 3 years after cutoff. Transfer to National Archives and Records Administration 20 years after cutoff. Retain an electronic copy until no longer needed. (Allegation records will be managed in the corresponding Investigation Case File).

Referred Allegations are retained under the National Archives and Records Administration's approved schedule, N1–431–10–002, item 2.a.ii. Cut off allegation file at the end of the fiscal year when the issue described in the Referral Letter is resolved. Hold allegation file in the OIG for a minimum of 2 years after cutoff. Destroy 10 years after cutoff.

Closed Allegations are retained under the National Archives and Records Administration's approved schedule, N1–431–10–002, item 2.a.iii. Cut off allegation files at the end if the fiscal year in which the allegation is closed. Destroy the allegation file 5 years after cutoff.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Access to the automated Investigative Database Program is password protected. Index card files for older cases (1970–1989) are maintained in secure office facilities. Both the Allegations Tracking System and the Investigative Management System are accessible from terminals that are double-password-protected. Paper files backing up the automated systems and older case reports and work papers are maintained in approved security containers and locked filing cabinets in a locked room; associated indices, records, diskettes, tapes, etc., are stored in locked metal filing cabinets, safes, storage rooms, or similar secure facilities. All records in this system are available only to authorized personnel who have a need to know and whose duties require access to the information.

RECORD ACCESS PROCEDURES:

Same as ''Notification procedures.'' Information classified under Executive Order 12958 will not be disclosed. Information received in confidence will be maintained under the Inspector General Act, 5 U.S.C. app. 3, and the Commission's Policy Statement on Confidentiality, Management Directive 8.8, ''Management of Allegations.''

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:

Under 5 U.S.C. 552a(j)(2), the Commission has exempted this system of records from subsections (c)(3) and (4), (d)(1)–(4), (e)(1)–(3), (5), and (8), and (g) of the Act. This exemption applies to information in the system that relates to criminal law enforcement and meets the criteria of the (j)(2) exemption. Under 5 U.S.C. 552a(k)(1), (k)(2), (k)(5), and (k)(6), the Commission has exempted portions of this system of records from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f).

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Disclosure Pursuant to 5 U.S.C. 552a(b)(12): Disclosure of information to a consumer reporting agency is not considered a routine use of records. Disclosures may be made from this system to ''consumer reporting agencies'' as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f) (1970)) or the Federal Claims Collection Act of 1966, as amended (31 U.S.C. 3701(a)(3) (1996)).

SYSTEM NAME AND NUMBER:

Official Personnel Training Records—NRC 19.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Primary system located at the NRC's current contractor facility on behalf of the Office of the Chief Human Capital Officer, NRC, Two White Flint North, 11545 Rockville Pike, Rockville, Maryland.

The Office of the Inspector General (OIG) employee files are located with the OIG at NRC, One White Flint North, 11555 Rockville Pike, Rockville, Maryland.

Duplicate system—Duplicate systems exist, in part, at the Technical Training Center, Regional Offices, and within the organization where the NRC employee works, at the locations listed in Addendum I, Parts 1 and 2.

SYSTEM MANAGER(S):

Associate Director for Training and Development, Office of the Chief Human Capital Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001. For OIG employee records: Director, Resource Management and Operations Support, Office of the Inspector General, Washington, DC 20555–0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 3396; 5 U.S.C. 4103; Executive Order (E.O.) 9397, as amended by E.O. 13478; E.O. 11348, as amended by E.O. 12107; 5 CFR parts 410 and 412.

PURPOSE(S) OF THE SYSTEM:

This record system will collect, and document training given to NRC employees, contractors, and others who are provided NRC training. This system will provide NRC with a means to track the particular training that is provided, identify training trends, monitor and track the expenditure of training, schedule training classes and programs, schedule instructors, track training items issued to students, assess the effectiveness of training, identify patterns, respond to requests for information related to the training of NRC personnel and other individuals.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who applied or were selected for NRC, other Government, or non-Government training courses or programs.

CATEGORIES OF RECORDS IN THE SYSTEM:

These records contain information relating to an individual's educational background and training courses including training requests and authorizations, evaluations, supporting documentation, and other related personnel information, including but not limited to, an individual's name,

address, telephone number, position title, organization, and grade.

RECORD SOURCE CATEGORIES:

Information is provided by the subject individual, the employee's supervisor, and training groups, agencies, or educational institutions and learning activities.

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. Information may be extracted from the records and made available to the Office of Personnel Management; other Federal, State, and local government agencies; educational institutions and training facilities for purposes of enrollment and verification of employee attendance and performance;

b. 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;

c. 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;

d. 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;

e. 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

f. 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 in file folders and on electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Information is accessed by name, user identification number, course number, or course session number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained under the National Archives and Records Administration's General Records Schedule 2.6: Employee Training Records, Item 010, Non-mission employees training program records. Destroy when 3 years old, or 3 years after superseded or obsolete, whichever is appropriate, but longer retention is authorized if required for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Electronic records are maintained in a password protected computer system. Paper is maintained in lockable file cabinets and file rooms. Access to and use of these records is limited to those persons whose official duties require such access, with the level of access controlled by roles and responsibilities.

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.

NRC–20 (Rescinded.)

RESCINDMENT OF SYSTEM OF RECORDS NOTICE:

SYSTEM NAME AND NUMBER:

Official Travel Records—NRC 20.

SYSTEM MANAGER:

Chief, Travel Operations Branch, Division of the Controller, Office of the Chief Financial Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001. For passport and visa records: Chief, International Operations Branch, Office of International Programs, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

HISTORY:

These notices were last published in the **Federal Register** on November 17, 2016 (81 FR 81320).

SYSTEM NAME AND NUMBER:

Payroll Accounting Records—NRC 21.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Primary system—Division of the Comptroller, Office of the Chief Financial Officer, NRC, Two White Flint North, 11545 Rockville Pike, Rockville, Maryland. NRC has an interagency agreement with the Department of the Interior's Interior Business Center (DOI/IBC), Federal Personnel/Payroll System (FPPS), in Denver, Colorado, to maintain electronic personnel information and perform payroll processing activities for its employees as of November 2, 2003.

Duplicate system—Duplicate systems exist, in part, within the organization where the employee actually works for administrative purposes, at the locations listed in Addendum I, Parts 1 and 2.

SYSTEM MANAGER(S):

Chief, Financial Services and Operations Branch, Division of the Comptroller, Office of the Chief Financial Officer, U.S. Nuclear

Regulatory Commission, Washington, DC 20555–0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

26 CFR 31.6011(b)–2, 31.6109–1; 5 U.S.C. 6334; 5 U.S.C. part III, subpart D; 31 U.S.C. 716; 31 U.S.C., subtitle III, chapters 35 and 37; Executive Order (E.O.) 9397, as amended by E.O. 13478.

PURPOSE(S) OF THE SYSTEM:

The purpose of this system is to ensure proper payment of salary and benefits to NRC personnel, and to track time worked, leave, or other absences for reporting and compliance purposes.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Current and former NRC employees, including special Government employees (*i.e.,* consultants).

CATEGORIES OF RECORDS IN THE SYSTEM:

Pay, leave, benefit enrollment and voluntary allowance deductions, and labor activities, which includes, but is not limited to, an individual's name and social security number.

RECORD SOURCE CATEGORIES:

Information in this system of records is obtained from sources, including but not limited to, the individual to whom it pertains, the Office of the Chief Human Capital Officer and other NRC officials, and other agencies and entities.

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

In accordance with an interagency agreement the NRC may disclose records to the DOI/IBC FPPS in order to effect all financial transactions on behalf of the NRC related to employee pay. Specifically, the DOI/IBC's FPPS may affect employee pay or deposit funds on behalf of NRC employees, and/or it may withhold, collect or offset funds from employee salaries as required by law or as necessary to correct overpayment or amounts due.

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; or, where determined to be appropriate and necessary, the NRC may authorize DOI/IBC to make the disclosure:

a. For transmittal of data to U.S. Treasury to effect issuance of paychecks to employees and consultants and distribution of pay according to employee directions for savings bonds, allotments, financial institutions, and other authorized purposes including the withholding and reporting of Thrift Savings Plan deductions to the Department of Agriculture's National Finance Center;

b. For reporting tax withholding to Internal Revenue Service and appropriate State and local taxing authorities;

c. For FICA and Medicare deductions to the Social Security Administration;

d. For dues deductions to labor unions;

e. For withholding for health insurance to the insurance carriers by the Office of Personnel Management;

f. For charity contribution deductions to agents of charitable institutions;

g. For annual W–2 statements to taxing authorities and the individual;

h. For transmittal to the Office of Management and Budget for financial reporting;

i. For withholding and reporting of retirement, tax levies, bankruptcies, garnishments, court orders, re-employed annuitants, and life insurance information to the Office of Personnel Management;

j. For transmittal of information to State agencies for unemployment purposes;

k. For transmittal to the Office of Child Support Enforcement, Administration for Children and Families, Department of Health and Human Services Federal Parent Locator System and Federal Tax Offset System for use in locating individuals and identifying their income sources to establish paternity, establish and modify orders of support, and for enforcement action;

l. For transmittal to the Office of Child Support Enforcement for release to the Social Security Administration for verifying social security numbers in connection with the operation of the Federal Parent Locator System by the Office of Child Support Enforcement;

m. For transmittal to the Office of Child Support Enforcement for release to the Department of Treasury for the purpose of administering the Earned Income Tax Credit Program (Section 32, Internal Revenue Code of 1986) and verifying a claim with respect to employment in a tax return;

n. To the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. 2904 and 2906;

o. Time and labor data are used by the NRC as a project management tool in various management records and reports (*i.e.,* work performed, work load projections, scheduling, project assignments, budget), and for identifying reimbursable and fee billable work performed by the NRC;

p. 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;

q. 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;

r. 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;

s. 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;

t. 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;

u. 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;

v. 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

w. 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:

Information is maintained on electronic media (stored in memory, on disk, and magnetic tape), on microfiche, and in paper copy.

Electronic payroll, time, and labor records prior to November 2, 2003, are maintained in the Human Resources Management System (HRMS), the PAY PERS Historical database reporting system, and on microfiche at NRC. Electronic payroll records from November 2, 2003, forward are maintained in the DOI/IBC's FPPS in Denver, Colorado. Time and labor records are maintained in the HRMS at NRC.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Information is accessed by employee identification number, name and social security number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained under the National Archives and Records Administration's General Records Schedule 2.4: Employee Compensation and Benefits Records, Item 010, Records used to calculate payroll, arrange paycheck deposit, and change previously issued paychecks. Destroy 2 year after employee separation or retirement, but longer retention is authorized if required for business use. Records are also retained under General Records Schedule 2.4, item 020, Tax withholding and adjustment documents. Destroy 4 years after superseded or obsolete, but longer retention is authorized if required for business use. Records are also retained under General Records Schedule 2.4, item 030, Time and attendance records. Destroy after GAO audit or when 3 years old, whichever is sooner. Records are also retained under General Records Schedule 2.4, item 040, Agency payroll record for each pay period. Destroy when 56 years old. Records are also retained under General Records Schedule 2.4, item 050, Wage and tax statements. Destroy when 4 years old, but longer retention is authorized if required for business use. Payroll program administrative records are retained under General Records Schedule 2.4, item 060, Administrative correspondence between agency and payroll processor, and system reports used for agency workload and or personnel management purposes. Destroy when 2 years old, but longer retention is authorized if required for business use. Payroll system reports providing fiscal information on agency payroll are retained under General Records Schedule 2.4, item 061. Destroy when 3 years old or after GAO audit, whichever comes sooner, but longer retention is authorized if required for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records are maintained in buildings where access is controlled by a security guard force. File folders, microfiche, tapes, and disks, including backup data, are maintained in secured locked rooms and file cabinets after working hours. All records are in areas where access is controlled by keycard and is limited to NRC and contractor personnel who need the information to perform their official duties. Access to computerized records requires use of proper passwords and user identification codes.

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.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Disclosure pursuant to 5 U.S.C. 552a(b)(12): Disclosures of information to a consumer reporting agency are not considered a routine use of records. Disclosures may be made from this system to ''consumer reporting agencies'' as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f) (1970)) or the Federal Claims Collection Act of 1966, as amended (31 U.S.C. 3701(a)(3) (1996)).

NRC–22 (Rescinded.)

RESCINDMENT OF SYSTEM OF RECORDS NOTICE:

SYSTEM NAME AND NUMBER:

Personnel Performance Appraisals—NRC 22.

SYSTEM MANAGER:

Associate Director for Human Resources Operations and Policy, Office of the Chief Human Capital Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001. For OIG employees: Director, Resource Management and Operations Support, Office of the Inspector General, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001. For Regional personnel: Regional Personnel Officers at the appropriate Regional Office I–IV listed in Addendum I, Part 2.

HISTORY:

These notices were last published in the **Federal Register** on November 17, 2016 (81 FR 81320).

SYSTEM NAME AND NUMBER:

Office of Investigations Indices, Files, and Associated Records—NRC 23.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Primary system—Office of Investigations, NRC, One White Flint North, 11555 Rockville Pike, Rockville, Maryland.

Duplicate system—Records exist within the NRC Regional Office locations, listed in Addendum I, Part 2, during an active investigation.

SYSTEM MANAGER(S):

Director, Office of Investigations, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

42 U.S.C. 2035(c); 42 U.S.C. 2201(c); and 42 U.S.C. 5841; 10 CFR 1.36.

PURPOSE(S) OF THE SYSTEM:

NRC OI uses records and information collected and maintained in this system to receive and adjudicate allegations of violations of criminal, civil, and administrative laws and regulations relating to NRC programs, operations, and employees, as well as contractors and other individuals and entities associated with NRC; monitor complaint and investigation assignments, status, disposition, and results; manage investigations and information provided during the course of such investigations; audit actions taken by NRC management regarding employee misconduct and other allegations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals and entities referred to in potential or actual investigations and matters of concern to the Office of Investigations and correspondence on matters directed or referred to the Office of Investigations.

CATEGORIES OF RECORDS IN THE SYSTEM:

Office of Investigations correspondence, cases, memoranda, materials including, but not limited to, investigative reports, confidential source information, correspondence to and from the Office of Investigations, memoranda, fiscal data, legal papers, evidence, exhibits, technical data, investigative data, work papers, and management information data.

RECORD SOURCE CATEGORIES:

Information is obtained from sources including, but not limited to, NRC officials, employees, and licensees; Federal, State, local, and foreign agencies; and other persons.

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 persons or entities mentioned therein if the disclosure is compatible with the purpose for which the record was collected under the following routine uses:

a. A record from this system of records may be disclosed as a routine use to a Federal, State, local, or foreign agency or to an individual or organization if the disclosure is reasonably necessary to elicit information or to obtain the cooperation of a witness or an informant;

b. A record relating to an investigation or matter falling within the purview of the Office of Investigations may be disclosed as a routine use to the referring agency, group, organization, or individual;

c. A record relating to an individual held in custody pending arraignment, trial, or sentence, or after conviction, may be disclosed as a routine use to a Federal, State, local, or foreign prison, probation, parole, or pardon authority, to any agency or individual concerned with the maintenance, transportation, or release of such an individual;

d. A record in the system of records relating to an investigation or matter may be disclosed as a routine use to a foreign country under an international treaty or agreement;

e. A record from this system of records may be disclosed as a routine use to a Federal, State, local, or foreign law enforcement agency to assist in the general crime prevention and detection efforts of the recipient agency or to provide investigative leads to the agency;

f. 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;

g. 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;

h. 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;

i. 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;

j. 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;

k. 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;

l. 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

m. 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:

Information maintained on paper, photographs, audio/video tapes, and electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Information retrieved by document text and/or case number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records for this system are scheduled using NRC's NUREG 0910 Revision 4 and the National Archives and Records Administration's approved scheduled N1–431–01–001 for the Office of Investigations.

Official investigation case files created by field investigators and maintained at regional field offices selected for permanent retention are scheduled under NUREG 0910, Revision 4, 2.16.4.a. Cut off files when case is closed. Hold in field office for 6 months then forward to headquarters (HQ) for processing. HQ will combine with its files, hold for 2 years. Transfer closed cases in 10 year blocks to the National Archives. Other case files that do not meet the criteria for permanent retention are scheduled under NUREG 0910, Revision 4, 2.16.4.b. Cut off files when case is closed. Hold in field office for 6 months then forward to HQ for processing. HQ will combine with its files, hold for 2 years. Destroy 20 years after cases are closed. HQ copy is scheduled under NUREG 0910, Revision 4, 2.16.4.c. Cut off files when case is closed. Combine with field office files and process in accordance with a and b above. Electronic input source records used to create paper records that are files in the investigation files are scheduled under NUREG 0910, Revision 4, 2.16.4.d. Create paper record of the electronic document on the day created or received or as soon as practical and file in appropriate official files. Destroy electronic version immediately after creating official record copy or when no longer needed for reference or updating, whichever is later.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Hard copy files maintained in approved security containers and locking filing cabinets. All records are under visual control during duty hours and are available only to authorized personnel who have a need to know and whose duties require access to the information. The electronic management information system is operated within the NRC's secure LAN/WAN system. Access rights to the system only available to authorized personnel.

RECORDS ACCESS PROCEDURES:

Same as ''Notification procedures.'' Information classified under Executive Order 12958 will not be disclosed. Information received in confidence will be maintained under the Commission's Policy Statement on Confidentiality, Management Directive 8.8, ''Management of Allegations,'' and the procedures covering confidentiality in Chapter 7 of the Office of Investigations Procedures Manual and will not be disclosed to the extent that disclosure would reveal a confidential source.

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:

Pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(6), the Commission has exempted portions of this system of records from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f).

NRC–24 (Rescinded.)

SYSTEM NAME AND NUMBER:

Oral History Program—NRC 25.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Office of the Secretary, NRC, One White Flint North, 11555 Rockville Pike, Rockville, Maryland.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

42 U.S.C. 2161(b) and 44 U.S.C. 3301.

PURPOSE(S) OF THE SYSTEM:

Recorded interviews and transcribed scripts of interviews for providing a history of the nuclear regulatory program.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who volunteer to be interviewed for the purpose of providing information for a history of the nuclear regulatory program.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records consist of recorded interviews and, as needed, transcribed scripts of the interviews.

RECORD SOURCE CATEGORIES:

Information in this system of records is obtained from interviews granted on a voluntary basis to the Historian.

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. For incorporation in publications on the history of the nuclear regulatory program;

b. To provide information to historians and other researchers;

c. 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

d. 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:

Maintained on electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Information is accessed by the name of the interviewee.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Narrative Histories are retained under NRC's NUREG 0910 Revision 4—(2.22.7.a(1)). Transfer to the National Archives and Records Administration when 20 years old. ADAMS PDFs and TIFFs are retained under NRC's NUREG 0910 Revision 4—(2.22.7.a(4)). Cut off electronic files at close of fiscal year. Transfer to the National Archives and Records Administration 5 years after cutoff. Destroy NRC copy 20 years after transfer.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Maintained on an access restricted drive. Access to and use of these records is limited to those authorized by the Historian or a designee.

SYSTEM MANAGER(S):

NRC Historian, Office of the Secretary, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

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.

SYSTEM NAME AND NUMBER:

Transit Subsidy Benefits Program Records—NRC 26.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Facility Operations and Space Management Branch, Office of Administration, NRC, Two White Flint North, 11545 Rockville Pike, Rockville, Maryland.

SYSTEM MANAGER(S):

Chief, Facility Operations and Space Management Branch, Division of Facilities and Security, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 7905; 26 U.S.C. 132; 31 U.S.C. 3511; 41 CFR 102–74.210; 41 CFR subtitle F; 41 CFR 102–71.20; Executive Order (E.O.) 9397, as amended by E.O. 13478; E.O. 13150.

PURPOSE(S) OF THE SYSTEM:

The information contained in this system is used to enroll employees in the Transit Subsidy Program.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

NRC employees who apply for subsidized mass transit costs.

CATEGORIES OF RECORDS IN THE SYSTEM:

The records consist of an individual's application to participate in the program which includes, but is not limited to, the applicant's name, home address, office telephone number, and information regarding the employee's commuting schedule and mass transit system(s) used.

RECORD SOURCE CATEGORIES:

NRC employees.

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 statistical reports to the city, county, State, and Federal government agencies;

b. To provide the basis for program approval and issue monthly subsidies;

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 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;

e. 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;

f. 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;

g. 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

h. 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 in file folders and on electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Accessed by name and smart trip card.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained under the National Archives and Records Administration's General Records Schedule 2.4: Employee Compensation and Benefit Records, Item 130, Transportation subsidy program administrative records. Destroy when 3 years old, but longer retention is authorized if required for business use. Records are also retained under General Records Schedule 2.4, item 131, Transportation subsidy program individual case files. Destroy 2 years after employee participation concludes, but longer retention is authorized if required for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Paper records are maintained in locked file cabinets under visual control of the Facility Operations and Space Management Branch staff. Computer files are maintained on a hard drive, access to which is password protected. Access to and use of these records is limited to those persons whose official duties require access.

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.

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.

NRC–28 (Rescinded.)

RESCINDMENT OF SYSTEM OF RECORDS NOTICE:

SYSTEM NAME AND NUMBER:

Merit Selection Records—NRC 28.

SYSTEM MANAGER:

Associate Director for Human Resources Operations and Policy, Office of Chief Human Capital Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001. For Regional personnel: Regional Personnel Officer at the appropriate Regional Office I–IV listed in Addendum I, Part 2. For applicants to the Honor Law Graduate Program—Honor Law Graduate Program Coordinator, Office of the General Counsel, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001. For OIG personnel: Personnel Officer, Office of the Inspector General, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

HISTORY:

These notices were last published in the **Federal Register** on November 17, 2016 (81 FR 81320).

NRC–29 (Rescinded.)

NRC–30 (Rescinded.)

NRC–31 (Rescinded.)

SYSTEM NAME AND NUMBER:

Office of the Chief Financial Officer Financial Transactions and Debt Collection Management Records—NRC 32.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Office of the Chief Financial Officer, NRC, Two White Flint North, 11545 Rockville Pike, Rockville, Maryland. NRC has an inter-agency agreement with the U.S. Treasury, Administrative Resource Center (ARC), Parkersburg, WV, as a Federal service provider for transactional services in the NRC core financial system since March 2018.

Other NRC systems of records contain information that may duplicate some of

the records in this system. These other systems include, but are not limited to:

NRC–5, Contracts Records—NRC;

NRC–10, Freedom of Information Act (FOIA) and Privacy Act (PA) Request Records—NRC;

NRC–18, Office of the Inspector General (OIG) Investigative Records—NRC;

NRC–19, Official Personnel Training Records—NRC;

NRC–21, Payroll Accounting Records—NRC; and

NRC–41, Tort Claims and Personal Property Claims Records—NRC.

SYSTEM MANAGER:

Comptroller, Division of the Comptroller, Office of the Chief Financial Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 552a; 5 U.S.C. 5514; 15 U.S.C. 1681; 26 U.S.C. 6103; 31 U.S.C. chapter 37; 31 U.S.C. 6501–6508; 42 U.S.C. 2201; 42 U.S.C. 5841; 31 CFR 900–904; 10 CFR parts 15, 16, 170, 171; Executive Order (E.O.) 9397, as amended by E.O. 13478; and E.O. 12731.

PURPOSE(S) OF THE SYSTEM:

Financial Transactions and Debt Collection.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals covered are those to who the NRC owes/owed money, those who receive/received a payment from NRC, and those who owe/owed money to the United States. Individuals receiving payments include, but are not limited to, current and former employees, contractors, consultants, vendors, and others who travel or perform certain services for NRC. Individuals owing money include, but are not limited to, those who have received goods or services from NRC for which there is a charge or fee (NRC licensees, applicants for NRC licenses, Freedom of Information Act requesters, etc.) and those who have been overpaid and owe NRC a refund (current and former employees, contractors, consultants, vendors, etc.).

CATEGORIES OF RECORDS IN THE SYSTEM:

Information in the system includes, but is not limited to, names, addresses, telephone numbers, Social Security Numbers (SSN), employee identification number (EIN), Taxpayer Identification Numbers (TIN), Individual Taxpayer Identification Numbers (ITIN), Data Universal Numbering System (DUNS) number, fee categories, application and license numbers, contract numbers, vendor numbers, amounts owed, background and supporting documentation, correspondence concerning claims and debts, credit reports, and billing and payment histories. The overall agency accounting system contains data and information integrating accounting functions such as general ledger, funds control, travel, accounts receivable, accounts payable, property, and appropriation of funds. Although this system of records contains information on corporations and other business entities, only those records that contain information about individuals that is retrieved by the individual's name or other personal identifier are subject to the Privacy Act.

RECORD SOURCE CATEGORIES:

Record source categories include, but are not limited to, individuals covered by the system, their attorneys, or other representatives; NRC; collection agencies or contractors; employing agencies of debtors; and Federal, State and local agencies.

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

In accordance with an interagency agreement, the NRC may disclose records to Treasury ARC as a Federal service provider for transactional services in the NRC core financial system. 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 or, where determined to be appropriate and necessary, the NRC may authorize Treasury ARC to make the disclosure:

a. To debt collection contractors (31 U.S.C. 3718) or to other Federal agencies such as the Department of the Treasury (Treasury) and DOI for the purpose of collecting and reporting on delinquent debts as authorized by the Debt Collection Act of 1982 or the Debt Collection Improvement Act (DCIA) of 1996 and the Digital Accountability and Transparency Act (DATA) of 2014;

b. To Treasury; the Defense Manpower Data Center, Department of Defense; the United States Postal Service; government corporations; or any other Federal, State, or local agency to conduct an authorized computer matching program in compliance with the Privacy Act of 1974, as amended, to identify and locate individuals, including Federal employees, who are delinquent in their repayment of certain debts owed to the U.S. Government, including those incurred under certain programs or services administered by the NRC, in order to collect debts under common law or under the provisions of the Debt Collection Act of 1982 or the Debt Collection Improvement Act of 1996 and DATA of 2014 which include by voluntary repayment, administrative or salary offset, and referral to debt collection contractors;

c. To the Department of Justice, United States Attorney Treasury ARC, or other Federal agencies for further collection action on any delinquent account when circumstances warrant;

d. To credit reporting agencies/credit bureaus for the purpose of either adding to a credit history file or obtaining a credit history file or comparable credit information for use in the administration of debt collection. As authorized by the DCIA, NRC may report current (not delinquent) as well as delinquent consumer and commercial debt to these entities in order to aid in the collection of debts, typically by providing an incentive to the person to repay the debt timely;

e. To any Federal agency where the debtor is employed or receiving some form of remuneration for the purpose of enabling that agency to collect a debt owed the Federal Government on NRC's behalf by counseling the debtor for voluntary repayment or by initiating administrative or salary offset procedures, or other authorized debt collection methods under the provisions of the Debt Collection Act of 1982 or the DCIA of 1996. Under the DCIA, NRC may garnish non-Federal wages of certain delinquent debtors so long as required due process procedures are followed. In these instances, NRC's notice to the employer will disclose only the information that may be necessary for the employer to comply with the withholding order;

f. To the Internal Revenue Service (IRS) by computer matching to obtain the mailing address of a taxpayer for the purpose of locating such taxpayer to collect or to compromise a Federal claim by NRC against the taxpayer under 26 U.S.C. 6103(m)(2) and under 31 U.S.C. 3711, 3717, and 3718 or common law. Re-disclosure of a mailing address obtained from the IRS may be made only for debt collection purposes, including to a debt collection agent to facilitate the collection or compromise of a Federal claim under the Debt Collection Act of 1982 or the DCIA of 1996, except that re-disclosure of a mailing address to a reporting agency is for the limited purpose of obtaining a credit report on the particular taxpayer.

Any mailing address information obtained from the IRS will not be used or shared for any other NRC purpose or disclosed by NRC to another Federal, State, or local agency which seeks to locate the same taxpayer for its own debt collection purposes;

g. To refer legally enforceable debts to the IRS or to Treasury's Debt Management Services to be offset against the debtor's tax refunds under the Federal Tax Refund Offset Program;

h. To prepare W–2, 1099, or other forms or electronic submittals, to forward to the IRS and applicable State and local governments for tax reporting purposes. Under the provisions of the DCIA, NRC is permitted to provide Treasury with Form 1099–C information on discharged debts so that Treasury may file the form on NRC's behalf with the IRS. W–2 and 1099 Forms contain information on items to be considered as income to an individual, including certain travel related payments to employees, payments made to persons not treated as employees (*e.g.,* fees to consultants and experts), and amounts written-off as legally or administratively uncollectible, in whole or in part;

i. To banks enrolled in the Treasury Credit Card Network to collect a payment or debt when the individual has given his or her credit card number for this purpose;

j. To another Federal agency that has asked the NRC to effect an administrative offset under common law or under 31 U.S.C. 3716 to help collect a debt owed the United States. Disclosure under this routine use is limited to name, address, SSN, EIN, TIN, ITIN, and other information necessary to identify the individual; information about the money payable to or held for the individual; and other information concerning the administrative offset;

k. To Treasury or other Federal agencies with whom NRC has entered into an agreement establishing the terms and conditions for debt collection cross servicing operations on behalf of the NRC to satisfy, in whole or in part, debts owed to the U.S. Government. Cross servicing includes the possible use of all debt collection tools such as administrative offset, tax refund offset, referral to debt collection contractors, salary offset, administrative wage garnishment, and referral to the Department of Justice. The DCIA of 2014 requires agencies to transfer to Treasury or Treasury-designated Debt Collection Centers for cross servicing certain nontax debt over 120 days delinquent. Treasury has the authority to act in the Federal Government's best interest to service, collect, compromise, suspend, or terminate collection action under existing laws under which the debts arise;

l. Information on past due, legally enforceable nontax debts more than 120 days delinquent will be referred to Treasury for the purpose of locating the debtor and/or effecting administrative offset against monies payable by the Government to the debtor, or held by the Government for the debtor under the DCIA's mandatory, Government-wide Treasury Offset Program (TOP). Under TOP, Treasury maintains a database of all qualified delinquent nontax debts and works with agencies to match by computer their payments against the delinquent debtor database in order to divert payments to pay the delinquent debt. Treasury has the authority to waive the computer matching requirement for NRC and other agencies upon written certification that administrative due process notice requirements have been complied with;

m. For debt collection purposes, NRC may publish or otherwise publicly disseminate information regarding the identity of delinquent nontax debtors and the existence of the nontax debts under the provisions of the DCIA of 1996;

n. To the Department of Labor (DOL) and the Department of Health and Human Services (HHS) to conduct an authorized computer matching program in compliance with the Privacy Act of 1974, as amended, to match NRC's debtor records with records of DOL and HHS to obtain names, name controls, names of employers, addresses, dates of birth, and TINs. The DCIA requires all Federal agencies to obtain taxpayer identification numbers from each individual or entity doing business with the agency, including applicants and recipients of licenses, grants, or benefit payments; contractors; and entities and individuals owing fines, fees, or penalties to the agency. NRC will use TINs in collecting and reporting any delinquent amounts resulting from the activity and in making payments;

o. If NRC decides or is required to sell a delinquent nontax debt under 31 U.S.C. 3711(I), information in this system of records may be disclosed to purchasers, potential purchasers, and contractors engaged to assist in the sale or to obtain information necessary for potential purchasers to formulate bids and information necessary for purchasers to pursue collection remedies;

p. If NRC has current and delinquent collateralized nontax debts under 31 U.S.C. 3711(i)(4)(A), certain information in this system of records on its portfolio of loans, notes and guarantees, and other collateralized debts will be reported to Congress based on standards developed by the Office of Management and Budget, in consultation with Treasury;

q. To Treasury in order to request a payment to individuals owed money by the NRC;

r. To the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. 2904 and 2906;

s. 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;

t. 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;

u. 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;

v. 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;

w. 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;

x. 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;

y. 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

z. 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:

Information in this system is stored on paper, microfiche, and electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Automated information can be retrieved by name, SSN, TIN, DUNS number, license or application number, contract or purchase order number, invoice number, voucher number, and/or vendor code. Paper records are retrieved by invoice number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained under the National Archives and Records Administration's General Records Schedule 1.1: Financial Management and Reporting Records, Item 010, Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting as the Official record held in the office of record. Destroy 6 years after final payment or cancellation, but longer retention is authorized if needed for business use. Records related to Administrative claims by or against the United States are retained under General Records Schedule 1.1: Financial Management and Reporting Records, item 080. Destroy 7 years after final action, but longer retention is authorized if required for business use. Records used to calculate payroll, arrange paycheck deposit, and change previously issued paychecks are scheduled under General Records Schedule 2.4: Employee Compensation and Benefits Records, item 010. Destroy 2 year after employee separation or retirement, but longer retention is authorized if required for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records in the primary system are maintained in a building where access is controlled by a security guard force. Records are kept in lockable file rooms or at user's workstations in an area where access is controlled by keycard and is limited to NRC and contractor personnel who need the records to perform their official duties. The records are under visual control during duty hours. Access to automated data requires use of proper password and user identification codes by NRC or contractor personnel.

RECORDS 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.

DISCLOSURES TO CONSUMER REPORTING AGENCIES:

Disclosures Pursuant to 5 U.S.C. 552a(b)(12): Disclosures of information to a consumer reporting agency are not considered a routine use of records. Disclosures may be made from this system to ''consumer reporting agencies'' as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f) (1970)) or the Federal Claims Collection Act of 1966, as amended (31 U.S.C. 3701(a)(3) (1996)).

SYSTEM NAME AND NUMBER:

Special Inquiry Records—NRC 33.

SECURITY CLASSIFICATION:

Classified and Unclassified.

SYSTEM LOCATION:

Primary system—Special Inquiry Group, NRC, One White Flint North, 11555 Rockville Pike, Rockville, Maryland.

Duplicate system—Duplicate systems exist, in whole or in part, at the locations listed in Addendum I, Parts 1 and 2.

SYSTEM MANAGER(S):

Records Manager, Special Inquiry Group, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

42 U.S.C. 2051, 2052, 2201(c), (i) and (o).

PURPOSE(S) OF THE SYSTEM:

Investigation material for potential or actual concerns in connection with investigations of accidents or incidents at nuclear power plants or other nuclear facility, nuclear materials or an allegation regarding public health and safety.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals possessing information regarding or having knowledge of matters of potential or actual concern to the Commission in connection with the investigation of an accident or incident at a nuclear power plant or other nuclear facility, or an incident involving nuclear materials or an allegation regarding the public health and safety related to the NRC's mission responsibilities.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system consists of an alphabetical index file bearing individual names. The index provides access to associated records which are arranged by subject matter, title, or identifying number(s) and/or letter(s). The system incorporates the records of all Commission correspondence, memoranda, audit reports and data, interviews, questionnaires, legal papers, exhibits, investigative reports and data, and other material relating to or developed as a result of the inquiry, study, or investigation of an accident or incident.

RECORD SOURCE CATEGORIES:

The information in this system of records is obtained from sources including, but not limited to, NRC officials and employees; Federal, State,

local, and foreign agencies; NRC licensees; nuclear reactor vendors and architectural engineering firms; other organizations or persons knowledgeable about the incident or activity under investigation; and relevant NRC records.

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 information relating to an item which has been referred to the Commission or Special Inquiry Group for investigation by an agency, group, organization, or individual and may be disclosed as a routine use to notify the referring agency, group, organization, or individual of the status of the matter or of any decision or determination that has been made;

b. To disclose a record as a routine use to a foreign country under an international treaty or convention entered into and ratified by the United States;

c. To provide records relating to the integrity and efficiency of the Commission's operations and management and may be disseminated outside the Commission as part of the Commission's responsibility to inform the Congress and the public about Commission operations;

d. 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;

e. 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;

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 in file folders and electronic media. Documents are maintained in secured vault facilities.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Accessed by name (author or recipient), corporate source, title of document, subject matter, or other identifying document or control number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Permanent Records retained as General Program Correspondence Files (Subject Files) at the Office Director Level are scheduled under NUREG 0910 rev 4—2.18.5.a(1). Cut off at close of fiscal year. Hold for 2 years then retire to the Federal Records Center. Transfer to the National Archives and Records Administration when 20 years old. Permanent Nuclear Power Plant Docket Files are scheduled under NUREG 0910 Rev 4—2.18.11.a(1). Retain current fiscal year and last four years in NRC File Center. Closing date is the termination date following completion of decommissioning procedure. Transfer to the National Archives and Records Administration 20 years after termination of license.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

These records are located in locking filing cabinets or safes in a secured facility and are available only to authorized personnel whose duties require access.

RECORD ACCESS PROCEDURES:

Same as ''Notification procedures.'' Information classified under Executive Order 12958 will not be disclosed. Information received in confidence will not be disclosed to the extent that disclosure would reveal a confidential source.

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:

Pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(5), the Commission has exempted portions of this system of records from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f).

NRC–34 (Rescinded.)

SYSTEM NAME AND NUMBER:

Drug Testing Program Records—NRC 35.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Primary system—Division of Facilities and Security, Office of Administration, NRC, Two White Flint North, 11545 Rockville Pike, Rockville, Maryland.

Duplicate system—Duplicate systems exist in part at the NRC Regional office locations listed in Addendum I, Part 2 (for a temporary period of time); and at the current contractor testing laboratories, collection/evaluation facilities.

SYSTEM MANAGER(S):

Director, Division of Facilities and Security, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C 7301; 5 U.S.C. 7361–7363; 42 U.S.C. 2165; 42 U.S.C. 290dd; Executive Order (E.O.) 12564; 9397, as amended by E.O. 13478.

PURPOSE(S) OF THE SYSTEM:

This record system will maintain information gathered by and in the possession of NRC Drug Testing Program, used in verifying positive test results for illegal use of controlled substance, as well as collecting and maintaining evidence of possession, distribution, or trafficking of controlled substances.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

NRC employees, applicants, consultants, licensees, and contractors.

CATEGORIES OF RECORDS IN THE SYSTEM:

These records contain information regarding the drug testing program; requests for and results of initial, confirmatory and follow-up testing, if appropriate; additional information supplied by NRC employees, employment applicants, consultants, licensees, or contractors in challenge to positive test results; and written statements or medical evaluations of attending physicians and/or information regarding prescription or nonprescription drugs.

RECORD SOURCE CATEGORIES:

NRC employees, employment applicants, consultants, licensees, and contractors who have been identified for drug testing who have been tested; physicians making statements regarding medical evaluations and/or authorized prescriptions for drugs; NRC contractors for processing including, but not limited to, specimen collection, laboratories for analysis, and medical evaluations; and NRC staff administering the drug testing program to ensure the achievement of a drug-free workplace.

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 identify substance abusers within the agency;

b. To initiate counseling and/or rehabilitation programs;

c. To take personnel actions;

d. To take personnel security actions;

e. For statistical reporting purposes. Statistical reporting will not include personally identifiable information;

f. 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;

g. 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

h. 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. Specimens are maintained in appropriate environments.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are indexed and accessed by name, social security number, testing position number, specimen number, drug testing laboratory accession number, or a combination thereof.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Employee drug test plans, procedures, and scheduling records are retained under the National Archives and Records Administration's General Records Schedule 2.7: Employee Health and Safety Records, item 100. Destroy when 3 years old or when superseded or obsolete. Employee drug test acknowledgement of notice forms are retained under General Records Schedule 2.7, item 110. Destroy when employee separates from testing-designated position. Employee drug testing specimen records are retained under General Records Schedule 2.7, item 120. Destroy 3 years after date of last entry or when 3 years old, whichever is later. Employee drug test results (Positive Results) are retained under General Records Schedule 2.7, item 130. Destroy when employee leaves agency or when 3 years old, whichever is later. Employee drug test results (Negative results) are retained under General Records Schedule 2.7, item 131. Destroy when 3 years old.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records in use are protected to ensure that access is limited to those persons whose official duties require such access. Unattended records are maintained in NRC-controlled space in locked offices, locked desk drawers, or locked file cabinets. Stand-alone and network processing systems are password protected and removable media is stored in locked offices, locked desk drawers, or locked file cabinets when unattended. Network processing systems have roles and responsibilities protection and system security plans. Records at laboratory, collection, and evaluation facilities are stored with appropriate security measures to control and limit access to those persons whose official duties require such access.

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:

Pursuant to 5 U.S.C. 552a(k)(5), the Commission has exempted portions of this system of records from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f).

SYSTEM NAME AND NUMBER:

Employee Locator Records—NRC 36.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Primary system—Part 1: For Headquarters personnel: Office of Chief Human Capital Officer, NRC, Two White Flint North, 11545 Rockville Pike, Rockville, Maryland. For Regional personnel: Regional Offices I–IV at the locations listed in Addendum 1, Part 2.

Part 2: Operations Division, Office of the Chief Information Officer, NRC, Two White Flint North, 11545 Rockville Pike, Rockville, Maryland.

Part 3: Division of Administrative Services, Office of Administration, NRC, One White Flint North, 11555 Rockville Pike, Rockville, Maryland.

Duplicate system—Duplicate systems exist, in part, for Incident Response Operations within the Office of Nuclear Security and Incident Response, NRC, Two White Flint North, 11545 Rockville Pike, Rockville, Maryland, and at the NRC's Regional Offices, at the locations listed in Addendum I, Part 2.

Duplicate system—Duplicate systems may exist, in part, within the organization where an individual actually works, at the locations listed in Addendum I, Parts 1 and 2.

SYSTEM MANAGER(S):

Part 1: For Headquarters personnel: Associate Director for Human Resources Operations and Policy, Office of the Chief Human Capital Officer, U.S. Nuclear Regulatory Commission (NRC), Washington, DC 20555–0001; and for Regional personnel: Regional Personnel Officer at the Regional Offices listed in Addendum I, Part 2; Part 2: IT Specialist, Network/Infrastructure Services Branch, IT Services Development & Operations Division, Office of the Chief Information Officer, NRC, Washington, DC 20555–0001; Part 3: Mail Services Team Leader, Administrative Services Center, Division of Administrative Services, Office of Administration, NRC, Washington, DC 20555–0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

44 U.S.C. 3101, 3301; Executive Order (E.O.) 9397, as amended by E.O. 13478; and E.O. 12656.

PURPOSE(S) OF THE SYSTEM:

The purpose of this system is for NRC employees and contractor's accountability, to support NRC emergency response, and to contact designated persons in the event of an emergency.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

NRC employees and contractors.

CATEGORIES OF RECORDS IN THE SYSTEM:

These records include, but are not limited to, an individual's name, home address, office organization and location (building, room number, mail stop), telephone number (home, business, and cell), person to be notified in case of emergency (name, address, telephone number), and other related records.

RECORD SOURCE CATEGORIES:

Individual on whom the record is maintained; Employee Express; Enterprise Identity Hub (EIH), and other related records.

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 contact the subject individual's designated emergency contact in the case of an emergency;

b. To contact the subject individual regarding matters of official business;

c. To maintain the agency telephone directory (accessible from *www.nrc.gov*);

d. For internal agency mail services;

e. 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;

f. 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;

g. 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

h. 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:

Electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Information is accessed by name.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Mail, printing, and telecommunication service control records are retained under the National Archives and Records Administration's

General Records Schedule 5.5: Mail, Printing, and Telecommunications Service Management Records, item 020. Destroy when 1 year old or when superseded or obsolete, whichever is applicable, but longer retention is authorized if required for business use. Custom/client records are retained under General Records Schedule 6.5: Public Customer Service Records, item 020. Destroy when superseded, obsolete, or when customer requests the agency to remove the records.

Administrative records maintained in any agency office are retained under General Records Schedule 5.1: Common Office Records, item 010. Destroy when business use ceases.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Electronic records are password protected. Access to and use of these records is limited to those persons whose official duties require such access.

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.

SYSTEM NAME AND NUMBER:

Information Security Files and Associated Records—NRC 37.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Division of Security Operations, Office of Nuclear Security and Incident Response, NRC, One White Flint North, 11555 Rockville Pike, Rockville, Maryland.

SYSTEM MANAGER(S):

Director, Division of Security Operations, Office of Nuclear Security and Incident Response, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

42 U.S.C. 2161–2169 and 2201(i); Executive Order 13526; 10 CFR part 95.

PURPOSE(S) OF THE SYSTEM:

Keep track of NRC employees, contractors, consultants, licensees, and other cleared persons who have been granted classification authority and the classification decisions that they make.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals include present and former NRC employees, contractors, consultants, licensees, and other cleared persons.

CATEGORIES OF RECORDS IN THE SYSTEM:

These records include information regarding:

a. Personnel who are authorized access to specified levels, categories and types of information, the approving authority, and related documents; and

b. Names of individuals who classify and/or declassify documents (*e.g.,* for the protection of Classified National Security Information and Restricted Data) as well as information identifying the document.

RECORD SOURCE CATEGORIES:

NRC employees, contractors, consultants, and licensees, as well as information furnished by other Government agencies or their contractors.

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 prepare statistical reports for the Information Security Oversight Office;

b. 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;

c. 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;

d. 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;

e. 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;

f. 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;

g. 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;

h. 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

i. 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 in file folders and on electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Accessed by name and/or assigned number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained under the National Archives and Records Administration's, General Records Schedule 4.2: Information Access and Protection Records. FOIA, Privacy Act, and classified administrative records are retained under General Records Schedule 4.2, item 001. Destroy when 3 years old, but longer retention is authorized if needed for business use. Information access and protection tracking and control records are retained under General Records Schedule 4.2, item 030. Destroy 2 years after last form entry, reply, or submission; or when associated documents are declassified or destroyed; or when authorization expires; whichever is appropriate. Longer retention is authorized if required for business use. Access control records are retained under General Records Schedule 4.2, item 031. Destroy when superseded or obsolete, but longer retention is authorized if required for business use. Accounting for and control of access to classified and controlled unclassified records and records requested under FOIA, PA and MDR are retained under General Records Schedule 4.2, item 040. Destroy or delete 5 years after date of last entry, final adjudication by courts, or final action by agency (such as downgrading, transfer or destruction of related classified documents, or release of information from controlled unclassified status), as may apply, whichever is later; but longer retention is authorized if required for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Information maintained in locked buildings, containers, or security areas under guard and/or alarm protection, as appropriate. Records are processed only on systems approved for processing classified information or accessible through password protected systems for unclassified information. The classified systems are stand-alone systems located within secure facilities or with removable hard drives that are either stored in locked security containers or in alarmed vaults cleared for open storage of TOP SECRET information.

CONTESTING RECORD PROCEDURE:

Same as ''Notification procedures.''

RECORD ACCESS PROCEDURE:

Same as ''Notification procedures.'' Some information is classified under Executive Order 13526 and will not be disclosed. Other information has been received in confidence and will not be disclosed to the extent that disclosure would reveal a confidential source.

NOTIFICATION PROCEDURE:

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:

Pursuant to 5 U.S.C. 552a(k)(1) and (k)(5), the Commission has exempted portions of this system of records from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4), (G), (H), and (I), and (f).

SYSTEM NAME AND NUMBER:

Mailing Lists—NRC 38.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Primary system—Multimedia, Graphics and Supply & Distribution Branch, Division of Facilities and Securities, Office of Administration, NRC, 11545 Rockville Pike, Rockville, Maryland.

Duplicate system—Duplicate systems exist in whole or in part at the locations listed in Addendum I, Parts 1 and 2.

SYSTEM MANAGER(S):

Printing Services Specialist, Multimedia, Graphics and Supply & Distribution Branch, Division of Facilities and Securities, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

44 U.S.C. 3101, 3301.

PURPOSE(S) OF THE SYSTEM:

The system is maintained for the purpose of mailing informational literature or responses to those who request it; maintaining lists of individuals who attend meetings; and for other purposes for which mailing or contact lists may be created.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals, including NRC staff, with an interest in receiving information from the NRC.

CATEGORIES OF RECORDS IN THE SYSTEM:

Mailing lists include an individual's name and address; and title, occupation, and institutional affiliation, when applicable.

RECORD SOURCE CATEGORIES:

NRC staff, NRC licensees, and individuals expressing an interest in NRC activities and publications.

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. A record from this system of records may be disclosed as a routine use for distribution of documents to persons and organizations listed on the mailing list;

b. 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;

c. 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

d. 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 electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are accessed by company name, individual name, or file code identification number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Customer/client records are retained under the National Archives and Records Administration's General Records Schedule 6.5: Public Customer Service Records, Item 020. Delete when superseded, obsolete, or when customer requests the agency to remove the records.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Access to and use of these records is limited to those persons whose official duties require such access.

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.

SYSTEM NAME AND NUMBER:

Personnel Security Files and Associated Records—NRC 39.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Division of Facilities and Security, Office of Administration, NRC, Two White Flint North, Rockville, Maryland.

SYSTEM MANAGER(S):

Director, Division of Facilities and Security, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

42 U.S.C. 2011 *et seq.;* 42 U.S.C. 2165, 2201(i), 2201a, and 2284; 42 U.S.C. 5801 *et seq.;* Executive Order (E.O.) 9397, as amended by E.O. 13478; E.O. 10450, as amended; E.O. 10865, as amended; E.O. 13467; E.O. 13526; E.O. 13587; 10 CFR parts 10, 11, 14, 25, 50, 73, 95; OMB Circular No. A–130, Revised; 5 CFR parts 731, 732, and authorities cited therein.

PURPOSE(S) OF THE SYSTEM:

This record system will maintain information gathered by and in the possession of the NRC Division of Facilities and Security to maintain the NRC's Personnel Security and Insider Threat programs.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Persons including NRC employees, employment applicants, consultants, contractors, and licensees; other Government agency personnel, other persons who have been considered for an access authorization, special nuclear material access authorization, unescorted access to NRC buildings or nuclear power plants, NRC building access, access to Federal automated information systems or data, or participants in the criminal history program; aliens who visit NRC's facilities; and actual or suspected violators of laws administered by NRC.

CATEGORIES OF RECORDS IN THE SYSTEM:

These records contain information about individuals, which includes, but is not limited to, their name(s), address, date and place of birth, social security number, identifying information, citizenship, residence history, employment history, military history, financial history, foreign travel, foreign contacts, education, spouse/cohabitant and relatives, personal references, organizational membership, medical, fingerprints, criminal record, and security clearance history. These records also contain copies of personnel security investigative reports from other Federal agencies, summaries of investigative reports, results of Federal agency indices and database checks, records necessary for participation in the criminal history program, reports of personnel security interviews, clearance actions information (*e.g.,* grants and terminations), access approval/disapproval actions related to NRC building access or unescorted access to nuclear plants, or access to Federal automated information systems or data, violations of laws, reports of security infraction, insider threat program inquiry records including analysis, results, referrals, and/or mitigation actions, and other related personnel security processing documents.

RECORD SOURCE CATEGORIES:

NRC applicants, employees, contractors, consultants, licensees, visitors and others, as well as information furnished by other Government agencies or their contractors.

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

Information in these records may be used by the Division of Facilities and Security and on a need-to-know basis by appropriate NRC officials, Hearing Examiners, Personnel Security Review Panel members, Office of Personnel Management, Central Intelligence Agency, Office of the Director of National intelligence, and other Federal agencies under the following routine uses:

a. To determine clearance or access authorization eligibility;

b. To determine eligibility for access to NRC buildings or access to Federal automated information systems or data;

c. To certify clearance or access authorization;

d. To maintain the NRC personnel security program, including the Insider Threat Program;

e. To provide licensees information needed for unescorted access or access to safeguards information determinations;

f. 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;

g. 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;

h. 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;

i. 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;

j. 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;

k. 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;

l. 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

m. 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 maintained on paper, tapes, and electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Indexed and accessed by name, social security number, docket number, or a combination thereof.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Security administrative records are retained under the National Archives and Records Administration's General Records Schedule 5.6: Security Records, Item 010. Destroy when 3 years old, but longer retention is authorized if required for business use. Visitor processing records in areas requiring highest level security awareness are retained under General Records Schedule 5.6, item 110. Destroy when 5 years old, but longer retention is authorized if required for business use. Visitor processing records in all other facility security areas are retained under General Records Schedule 5.6, item 111. Destroy when 2 years old, but longer retention is authorized if required for business use. Personnel security and access clearance records of people issued clearances are retained under General Records Schedule 5.6, item 181. Destroy 5 years after employee or contractor relationship ends, but longer retention is authorized if required for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records in use are protected to ensure that access is limited to those persons whose official duties require such access. Unattended records are maintained in NRC-controlled space in locked offices, locked desk drawers, or locked file cabinets. Mass storage of records is protected when unattended by a combination lock and alarm system. Unattended classified records are protected in appropriate security containers in accordance with Management Directive 12.1.

NOTIFICATION PROCEDURE:

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.

RECORD ACCESS PROCEDURE:

Same as ''Notification procedures.'' Some information is classified under Executive Order 12958 and will not be disclosed. Other information has been received in confidence and will not be disclosed to the extent the disclosure would reveal a confidential source.

CONTESTING RECORD PROCEDURE:

Same as ''Notification procedures.''

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(5), the Commission has exempted portions of this system of records from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f).

SYSTEM NAME AND NUMBER:

Facility Security Access Control Records—NRC 40.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Primary system—Division of Facilities and Security, Office of Administration, NRC, Two White Flint North, 11545 Rockville Pike, Rockville, Maryland.

Duplicate system—Duplicate systems exist in part at NRC Regional Offices and the NRC Technical Training Center at the locations listed in Addendum I, Part 2.

SYSTEM MANAGER(S):

Director, Division of Facilities and Security, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

42 U.S.C. 2165–2169 and 2201; Executive Order (E.O.) 9397, as amended by E.O. 13478; E.O. 13462, as amended by E.O. 13516.

PURPOSE(S) OF THE SYSTEM:

Tracking issued NRC personal identification badges issued for access to NRC-controlled space and approved visitors to the NRC.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Current and former NRC employees, consultants, contractors, other Government agency personnel, and approved visitors.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system includes information regarding: (1) NRC personal identification badges issued for

continued access to NRC-controlled space; and (2) records regarding visitors to NRC. The records include, but are not limited to, an individual's name, social security number, electronic image, badge number, citizenship, employer, purpose of visit, person visited, date and time of visit, and other information contained on Government issued credentials.

RECORD SOURCE CATEGORIES:

Sources of information include NRC employees, contractors, consultants, employees of other Government agencies, and visitors.

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 control access to NRC classified information and to NRC spaces by human or electronic means;

b. Information (identification badge) may also be used for tracking applications within the NRC for other than security access purposes;

c. The electronic image used for the NRC employee personal identification badge may be used for other than security purposes only with the written consent of the subject individual;

d. 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;

e. 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;

f. 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;

g. 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;

h. 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;

i. 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;

j. 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

k. 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.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Information is indexed and accessed by individual's name, social security number, identification badge number, employer's name, date of visit, or sponsor's name.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

The National Archives and Records Administration's General Records Schedule 5.6 includes Security Records. Visitor processing records in areas requiring highest level security awareness, including areas designated by the interagency Security Committee as Facility Security Level V, are retained according to General Records Schedule 5.6, item 110. Destroy when 5 years old, but longer retention is authorized if required for business use. Visitor processing records in facility security areas not requiring highest level security awareness, including areas designated by the interagency Security Committee as Facility Security Levels I through IV, are retained under General Records Schedule 5.6, item 111. Destroy when 2 years old, but longer retention is authorized if required for business use. Indexes to personnel security case files are retained under General Records Schedule 5.6, item 190. Destroy when superseded or obsolete. Records of routine security operations are retained under General Records Schedule 5.6, item 090. Destroy when 30 days old, but longer retention is authorized if required for business use. Personal identification credentials and cards, including application and activation records, are retained according to General Records Schedule 5.6, item 120. Destroy mandatory and optional data elements housed in the agency identity management system and printed on the identification card 6 years after terminating an employee or contractor's employment, but longer retention is authorized if required for business use. Personnel suitability and eligibility investigative reports are retained according to General Records Schedule 5.6, item 170. Destroy in accordance with the investigating agency instruction. Reports and records created by agencies conducting investigations under delegated investigative authority are retained according to General Records Schedule 5.6, item 171. Destroy in accordance with delegated authority agreement or memorandum of understanding.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

All records are maintained in NRC-controlled space that is secured after normal duty hours or a security area under guard presence in a locked security container/vault. There is an approved security plan which identifies the physical protective measures and access controls (*i.e.,* passwords and software design limiting access based on each individual's role and responsibilities relative to the system) specific to each system.

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.

SYSTEM NAME AND NUMBER:

Tort Claims and Personal Property Claims Records—NRC 41.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Primary system—Office of the General Counsel, NRC, One White Flint North, 11555 Rockville Pike, Rockville, Maryland.

Duplicate system—Duplicate systems exist, in whole or in part, in the Office of the Chief Financial Officer, NRC, Two White Flint North, 11545 Rockville Pike, Rockville, Maryland, and at the locations listed in Addendum I, Parts 1 and 2. Other NRC systems of records, including but not limited to, NRC–18, ''Office of the Inspector General (OIG) Investigative Records—NRC and Defense Nuclear Facilities Safety Board (DNFSB), '' and NRC–32, ''Office of the Chief Financial Officer Financial Transactions and Debt Collection Management Records—NRC,'' may contain some of the information in this system of records.

SYSTEM MANAGER:

Assistant General Counsel for Administration, Office of the General Counsel, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Federal Tort Claims Act, 28 U.S.C. 2671 *et seq.;* Military Personnel and Civilian Employees' Claims Act, 31 U.S.C. 3721; 44 U.S.C. 3101.

PURPOSE(S) OF THE SYSTEM:

Claims with the NRC under the Federal Tort Claims Act or the Military Personnel and Civilian Employees' Claims Act.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who have filed claims with NRC under the Federal Tort Claims Act or the Military Personnel and Civilian Employees' Claims Act and individuals who have matters pending before the NRC that may result in a claim being filed.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system contains information relating to loss or damage to property and/or personal injury or death in which the U.S. Government may be liable. This information includes, but is not limited to, the individual's name, home address and phone number, work address and phone number, driver's license number, claim forms and supporting documentation, police reports, witness statements, medical records, insurance information, investigative reports, repair/replacement receipts and estimates, litigation documents, court decisions, and other information necessary for the evaluation and settlement of claims.

RECORD SOURCE CATEGORIES:

Information is obtained from a number of sources, including but not limited to, claimants, NRC employees involved in the incident, witnesses or others having knowledge of the matter, police reports, medical reports, investigative reports, insurance companies, and attorneys.

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, NRC may disclose information contained in a record 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 third parties, including claimants' attorneys, insurance companies, witnesses, potential witnesses, local police authorities where an accident occurs, and others who may have knowledge of the matter to the extent necessary to obtain information that will be used to evaluate, settle, refer, pay, and/or adjudicate claims;

b. To the Department of Justice (DOJ) when the matter comes within their jurisdiction, such as to coordinate litigation or when NRC's authority is limited, and DOJ advice or approval is required before NRC can award, adjust, compromise, or settle certain claims;

c. To the appropriate Federal agency or agencies when a claim has been incorrectly filed with NRC or when more than one agency is involved, and NRC makes agreements with the other agencies as to which one will investigate the claim;

d. To the Department of the Treasury to request payment of an award, compromise, or settlement of a claim;

e. Information contained in litigation records is public to the extent that the documents have been filed in a court or public administrative proceeding, unless the court or other adjudicative body has ordered otherwise. This public information, including information concerning the nature, status, and disposition of the proceeding, may be disclosed to any person, unless it is determined that release of specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

f. To the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. 2904 and 2906;

g. 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;

h. 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;

i. 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;

j. 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;

k. 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;

l. 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;

m. 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

n. 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:

Information in this system of records is stored on paper and computer media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Information is indexed and accessed by the claimant's name and/or claim number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records will be retained under the National Archives and Records Administration's General Records Schedules and the NRC NUREG 0910 Revision 4.

Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting, are retained according to General Records Schedule 1.1: Financial Management and Reporting Records, item 010 (''Official record held in the office of record''). Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use. Administrative claims by or against the United States are retained according to General Records Schedule 1.1, item 080. Destroy 7 years after final action, but longer retention is authorized if required for business use. Litigation Case Files including paper records created before April 1, 2000, are retained according to NRC's NUREG 0910, Revision 4, Part 2.12.7.a. Retire closed files 7 years after cases are closed. Transfer to the National Archives and Records Administration 20 years after cases are closed. ADAMS PDFs and TIFFs are retained according to NUREG 0910, Revision 4, Part 2.12.7.d. Cut off electronic files when case is closed. Transfer to the National Archives and Records Administration 2 years after cutoff. Destroy NRC copy 18 years after transferring records.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

The paper records are stored in locked file cabinets or locked file rooms and access is restricted to those agency personnel whose official duties and responsibilities require access. Automated records are protected by password.

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.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Disclosure Pursuant to 5 U.S.C. 552a(b)(12): Disclosure of information to a consumer reporting agency is not considered a routine use of records. Disclosures may be made from this system of records to ''consumer reporting agencies'' as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f) (1970)) or the Federal Claims Collection Act of 1966, as amended (31 U.S.C. 3701(a)(3) (1996)).

NRC–42 (Rescinded.)

RESCINDMENT OF SYSTEM OF RECORDS NOTICE:

SYSTEM NAME AND NUMBER:

Strategic Workforce Planning Records—NRC 42.

SYSTEM MANAGER:

Chief, Program Management, Human Capital Analysis Branch, Office of the Chief Human Capital Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

HISTORY:

These notices were last published in the **Federal Register** on November 17, 2016 (81 FR 81320).

SYSTEM NAME AND NUMBER:

Employee Health Center Records—NRC 43.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Primary system—Employee Health Center, NRC, One White Flint North, 11555 Rockville Pike, Rockville, Maryland.

Duplicate system—Duplicate systems exist, in part, at health care facilities operating under a contract or agreement with NRC for health-related services in the vicinity of each of NRC's Regional offices listed in Addendum I, Part 2. NRC's Regional offices may also maintain copies of occupational health records for their employees.

This system may contain some of the information maintained in other systems of records, including NRC–11,

''Reasonable Accommodation Records—NRC,'' NRC–44, ''Employee Fitness Center Records—NRC, and DOL/GOVT–1 ''Office of Worker's Compensation Programs, Federal Employee's Compensation Act File.''

SYSTEM MANGERS(S):

Technical Assistance Project Manager, Office of the Chief Human Capital Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 7901; Executive Order 9397, as amended by E.O. 13478.

PURPOSE(S) OF THE SYSTEM:

Maintaining health records for current and former NRC employees, consultants, contractors, other Government personnel, and anyone who may require emergency or first-aid treatment on NRC premises.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Current and former NRC employees, consultants, contractors, other Government personnel, and anyone on NRC premises who requires emergency or first-aid treatment.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system is comprised of records developed as a result of voluntary employee use of health services provided by the Health Center, and of emergency health services rendered by Health Center staff to individuals for injuries and illnesses suffered while on NRC premises. Specific information maintained on individuals may include, but is not limited to, their name, date of birth, and social security number; medical history and other biographical data; test reports and medical diagnoses based on employee health maintenance physical examinations or health screening programs (tests for single medical conditions or diseases); history of complaint, diagnosis, and treatment of injuries and illness rendered by the Health Center staff; immunization records; records of administration by Health Center staff of medications prescribed by personal physicians; medical consultation records; statistical records; daily log of patients; and medical documentation such as personal physician correspondence, test results submitted to the Health Center staff by the employee; and occupational health records. This system does not maintain records that are a result of a condition of employment, records and reports generated in relation to a Workers' Compensation claim, or records resulting from participation in an agency-sponsored health and wellness program. Such records are maintained in the government-wide system of records notice ''OPM/GOVT–10 Employee Medical File System Records.''

RECORD SOURCE CATEGORIES:

Information in this system of records is obtained from a number of sources including, but not limited to, the individual to whom it pertains; laboratory reports and test results; NRC Health Center physicians, nurses, and other medical technicians or personnel who have examined, tested, or treated the individual; the individual's coworkers or supervisors; other systems of records; the individual's personal physician(s); NRC Fitness Center staff; other Federal agencies; and other Federal employee health units.

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 refer information required by applicable law to be disclosed to a Federal, State, or local public health service agency concerning individuals who have contracted certain communicable diseases or conditions in an effort to prevent further outbreak of the disease or condition;

b. To disclose information to the appropriate Federal, State, or local agency responsible for investigation of an accident, disease, medical condition, or injury as required by pertinent legal authority;

c. To disclose information to the Office of Workers' Compensation Programs in connection with a claim for benefits filed by an employee;

d. To Health Center staff and medical personnel under a contract or agreement with NRC who need the information in order to schedule, conduct, evaluate, or follow up on physical examinations, tests, emergency treatments, or other medical and health care services;

e. To refer information to private physicians designated by the individual when requested in writing;

f. To the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. 2904 and 2906;

g. 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;

h. 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;

i. 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;

j. 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;

k. 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;

l. 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;

m. 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

n. 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 stored in file folders, on electronic media, and on file cards, logs, x-rays, and other medical reports and forms.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are retrieved by the individual's name, date of birth, and social security number, or any combination of those identifiers.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Clinic Scheduling Records are retained under the National Archives and Records Administration's General Records Schedule 2.7: Employee Health and Safety Records, Item 010. Destroy when 3 years old, but longer retention is authorized if required for business use. Short-term occupational individual medical case files are retained under General Records Schedule 2.7, item 061. Destroy 1 year after employee separation or transfer. Individual employee health case files created prior to establishment of the Employee Medical File system in 1986 are retained under General Records Schedule 2.7, item 062. Destroy 60 years after retirement to the NARA records storage facility. Non-occupational individual medical case files are retained under General Records Schedule 2.7, item 070. Destroy 10 years after the most recent encounter, but longer retention is authorized if needed for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records in the primary system are maintained in a building where access is controlled by a security guard force and entry to each floor is controlled by keycard. Records in the system are maintained in lockable file cabinets with access limited to agency or contractor personnel whose duties require access. The records are under visual control during duty hours. Access to automated data requires use of proper password and user identification codes by authorized personnel.

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; comply with the procedures contained in NRC's Privacy Act regulations, 10 CFR part 9; and provide their full name, any former name(s), date of birth, and Social Security number.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

SYSTEM NAME AND NUMBER:

Employee Fitness Center Records—NRC 44.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Primary system—Fitness Center, NRC, Two White Flint North, 11545 Rockville Pike, Rockville, Maryland.

Duplicate system—Regional offices, listed in Addendum I, Part 2, only maintain lists of their employees who receive subsidy from NRC for off-site fitness center memberships.

SYSTEM MANAGER(S):

Office of Chief Human Capital Officer Contracting Officer Representative, Office of the Chief Human Capital Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 7901; Executive Order (E.O.) 9397, as amended by E.O. 13478.

PURPOSE(S) OF THE SYSTEM:

Maintaining membership for the NRC Fitness Center.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

NRC employees who apply for membership at the Fitness Center, including current and former members.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system includes applications to participate in NRC's Fitness Center, information on an individual's degree of physical fitness and their fitness activities and goals; and various forms, memoranda, and correspondence related to Fitness Facilities membership and financial/payment matters. Specific information contained in the application for membership includes the employee applicant's name, gender, age, badge id, height, weight, and medical information, including a history of certain medical conditions; the name of the individual's personal physician and any prescription or over-the-counter drugs taken on a regular basis; and the name and address of a person to be notified in case of emergency.

RECORD SOURCE CATEGORIES:

Information in this system of records is principally obtained from the subject individual. Other sources of information include, but are not limited to, the NRC Fitness Center Director, staff physicians retained by the NRC, and the individual's personal physicians.

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 the individual listed as an emergency contact, in the event of an emergency;

b. To the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. 2904 or 2906;

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.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Information is indexed and accessed by an individual's name and/or NRC Badge ID number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Fitness Center records are currently unscheduled and must be retained until the National Archives and Records Administration approves a records disposition schedule for this material. Non-occupational health and wellness program records are retained according to the National Archives and Records Administration's General Records Schedule 2.7: Employee Health and Safety Records, item 080. Destroy 3 years after the project/activity or transaction is completed or superseded, but longer retention is authorized if needed for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records are maintained in a building where access is controlled by a security guard force. Access to the Fitness Center is controlled by keycard and bar code verification. Records in paper form are stored alphabetically by individuals' names in lockable file cabinets maintained in the NRC where access to the records is limited to agency and Fitness Center personnel whose duties require access. The records are under visual control during duty hours. Automated records are protected by screen saver. Access to automated data requires use of proper password and user identification codes. Only authorized personnel have access to areas in which information is stored.

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.

DISCLOSURES TO CONSUMER REPORTING AGENCIES:

Disclosures Pursuant to 5 U.S.C. 552a(b)(12): Disclosures of information to a consumer reporting agency are not considered a routine use of records. Disclosures may be made from this system to ''consumer reporting agencies'' as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f) (1970)) or the Federal Claims Collection Act of 1966, as amended (31 U.S.C. 3701(a)(3) (1996)).

SYSTEM NAME AND NUMBER:

Electronic Credentials for Personal Identity Verification—NRC 45.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Primary system—Office of the Chief Information Officer, NRC, White Flint North Complex, 11555 Rockville Pike, Rockville, Maryland, and current contractor facility.

Duplicate system—Duplicate systems may exist, in whole or in part, at the locations listed in Addendum I, Part 2.

SYSTEM MANAGER(S):

Director, Solutions Development and Operations Division, Office of the Chief Information Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; 42 U.S.C. 2165 and 2201(i); 44 U.S.C. 3501, 3504; Electronic Government Act of 2002, 44 U.S.C. chapter 36; Homeland Security Presidential Directive 12 (HSPD–12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; Executive Order (E.O.) 9397, as amended by E.O. 13478.

PURPOSE(S) OF THE SYSTEM:

Track and control PIV cards issued to persons entering and exiting the NRC facilities or using NRC systems; and Verify that all person entering federal

facilities, using Federal information resources, are authorized to do so;

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals covered are persons who have applied for the issuance of electronic credentials for signature, encryption, and/or authentication purposes; have had their credentials renewed, replaced, suspended, revoked, or denied; have used their credentials to electronically make contact with, retrieve information from, or submit information to an automated information system; or have corresponded with NRC or its contractor concerning digital services.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system contains information needed to establish and verify the identity of users, to maintain the system, and to establish accountability and audit controls. System records may include: (a) Applications for the issuance, amendment, renewal, replacement, or revocation of electronic credentials, including evidence provided by applicants or proof of identity and authority, and sources used to verify an applicant's identity and authority; (b) credentials issued; (c) credentials denied, suspended, or revoked, including reasons for denial, suspension, or revocation; (d) a list of currently valid credentials; (e) a list of currently invalid credentials; (f) a record of validation transactions attempted with electronic credentials; and (g) a record of validation transactions completed with electronic credentials.

RECORD SOURCE CATEGORIES:

The sources for information are the individuals who apply for electronic credentials, the NRC and contractors using multiple sources to verify identities, and internal system transactions designed to gather and maintain data needed to manage and evaluate the electronic credentials program.

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 agency electronic credential program contractors to compile and maintain documentation on applicants for verifying applicants' identity and authority to access information system applications; to establish and maintain documentation on information sources for verifying applicants' identities; to ensure proper management, data accuracy, and evaluation of the system;

b. To Federal authorities to determine the validity of subscriber digital certificates and other identity attributes;

c. To the National Archives and Records Administration (NARA) for records management purposes;

d. To a public data repository (*only name, email address, organization, and public key*) to facilitate secure communications using digital certificates;

e. 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;

f. 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;

g. 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;

h. 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;

i. 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;

j. 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;

k. 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

l. 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 stored electronically or on paper.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are retrievable by an individual's name, email address, certificate status, certificate number or credential number, certificate issuance date, or approval role.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained under the National Archives and Records Administration's, General Records Schedule 5.6: Security Records. Application and activation records for personal identification credentials and cards are retained under General Records Schedule 5.6, item 120. Destroy mandatory and optional data elements housed in the agency identity management system and printed on the identification card 6 years after

terminating an employee or contractor's employment, but longer retention is authorized if required for business use. Personnel identification cards are retained under General Records Schedule 5.6, item 121. Destroy after expiration, confiscation, or return. Local facility identification and card access records are retained under General Records Schedule 5.6, item 130. Destroy upon immediate collection once the temporary credential or card is returned for potential reissuance due to nearing expiration or not to exceed 6 months from time of issuance or when individual no longer requires access, whichever is sooner, but longer retention is authorized if required for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Technical, administrative, and personnel security measures are implemented to ensure confidentiality, integrity, and availability of the system data stored, processed, and transmitted. Hard copy documents are maintained in locking file cabinets. Electronic records are, at a minimum, password protected. Access to and use of these records is limited to those individuals whose official duties require access.

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 CLAIMS FOR THE SYSTEM:

None.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Disclosure of system records to consumer reporting systems is not permitted.

Addendum I—List of U.S. Nuclear Regulatory Commission Locations

Part 1—NRC Headquarters Offices

1. One White Flint North, 11555 Rockville Pike, Rockville, Maryland.

2. Two White Flint North, 11545 Rockville Pike, Rockville, Maryland.

Part 2—NRC Regional Offices

1. NRC Region I, 2100 Renaissance Boulevard, Suite 100, King of Prussia, Pennsylvania.

2. NRC Region II, Marquis One Tower, 245 Peachtree Center Avenue NE, Suite 1200, Atlanta, Georgia.

3. NRC Region III, 2443 Warrenville Road, Suite 210, Lisle, Illinois.

4. NRC Region IV, 1600 East Lamar Boulevard, Arlington, Texas.

5. NRC Technical Training Center, Osborne Office Center, 5746 Marlin Road, Suite 200, Chattanooga, Tennessee.

[FR Doc. 2019–27584 Filed 12–26–19; 8:45 am]

BILLING CODE 7590–01–P