This document is scheduled to be published in the
Federal Register on 2026-10-06 and available online at
https://www.federalregister.gov/d/2026-20438, and on
https://govinfo.gov

BILLING CODE 7590-01-P

NUCLEAR REGULATORY COMMISSION

[NRC-2026-2311]

Privacy Act of 1974; Systems of Records

AGENCY: Nuclear Regulatory Commission.

ACTION: Notice of modified systems of records; request for comment.

SUMMARY: Pursuant to the Privacy Act of 1974 and the Office of Management and Budget (OMB) Circular A-108, the U.S. Nuclear Regulatory Commission (NRC) is republishing 13 Privacy Act systems of records notices (SORNs) following a comprehensive review. Eight notices include only minor administrative updates, one is unchanged, and four systems—NRC 27, NRC 36, NRC 39, and NRC 40—contain substantive revisions requiring a 30-day public comment period. The updates modernize system descriptions, clarify authorities and system locations, and update categories of records and safeguards.

DATES: Submit comments on revisions and changes by **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**. 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; however, the NRC encourages electronic comment submission through the **Federal rulemaking website**:

- **Federal rulemaking website:** Go to https://www.regulations.gov and search for Docket ID NRC-2026-2311. Address questions about Docket IDs in Regulations.gov to Bridget Curran; telephone: 301-415-1003; email: Bridget.Curran@nrc.gov. For

technical questions, contact the individual listed in the “For Further Information Contact” section of this document.

- **Mail comments to**: Office of Nuclear Material Safety and Safeguards, Mail Stop: TWFN-5-A85, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, ATTN: Guidance and Publications Branch.
- **Obtaining Information and Submitting Comments:** Please refer to Docket ID NRC-2026-2311 when contacting the NRC about the availability of information for this action. The NRC encourages electronic comment submission through the Federal rulemaking website (https://www.regulations.gov). Please include Docket ID NRC-2026-2311 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 Agencywide Documents Access and Management System (ADAMS). The NRC does not routinely edit comment submissions to remove identifying or contact information.

If you are requesting or aggregating comments from others for submission to the NRC, then you should inform them 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. 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-2026-2311.

- **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 ADAMS Public Search." For problems with ADAMS, please contact the NRC's Public Document Room (PDR) reference staff at 1-800-397-4209, at 301-415-4737, or by email to PDR.Resource@nrc.gov.
- **NRC's PDR:** The PDR, where you may examine and order copies of publicly available documents, is open by appointment. To make an appointment to visit the PDR, please send an email to PDR.Resource@nrc.gov or call 1-800-397-4209 or 301-415-4737, between 8 a.m. and 4 p.m. eastern time (ET), Monday through Friday, except Federal holidays.

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: The NRC has conducted a comprehensive review of 13 of its Privacy Act systems of records in accordance with the Privacy Act of 1974 and OMB Circular A-108. As a result of this review, the NRC is republishing all 13 SORNs. Eight SORNs include only minor or administrative updates that do not meet the threshold for a new or altered system, and one SORN is being republished without changes. Four SORNs—NRC 27, NRC 36, NRC 39, and NRC 40—contain substantive revisions that meet the criteria for an altered system of records and are therefore being published for a 30-day public comment period.

The proposed updates modernize system descriptions, clarify authorities, update system locations to reflect current organizational structures and cloud environments, revise categories of records and sources, and update administrative, technical, and physical safeguards. The changes also ensure each SORN is in alignment with current NRC operations, cybersecurity requirements, and applicable National Archives and

Records Administration records schedules.

A report on these revisions has been sent to OMB, the Committee on Homeland Security and Governmental Affairs of U.S. Senate, and the Committee on Oversight and Accountability 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.

(Authority: 42 U.S.C. 2011 *et seq.*)

Dated: October 1, 2026.

For the Nuclear Regulatory Commission.

Garo Nalabandian,
Senior Agency Official for Privacy, Office of the Chief Information Officer.

Attachment – U.S. Nuclear Regulatory Commission Privacy Act Systems of Records

NRC Systems of Records

25 Oral History Program

26 Transit Subsidy Benefits Program

27 Radiation Exposure Information and Reporting System

33 Special Inquiry Records

35 Drug Testing Program Records

36 Employee Locator Records

37 Information Security Files and Associated Records

38 Mailing Lists

39 Personnel Security Files and Associated Records

40 Facility Security Access Control Records

44 Employee Fitness Center Records

45 Electronic Credentials for Personal Identity Verification

46 Health Emergency Records

These systems of records are maintained by the NRC and contain personal information about individuals that 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:

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 other types of 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) the NRC suspects or has confirmed that there has been a breach of the system of records, (2) the NRC has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the 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 will be retained under NRC's approved schedule found in the NUREG 0910 version 4 at 2.22.7.a(1): Record copy maintained by the NRC Deputy Secretary. Permanent. Transfer to the National Archives when 20 years old. (Paper records created before 4/1/2000. ADAMS PDF files and TIFF files (2.22.7.a(4)) are cutoff at the close of the fiscal year. Transfer to the National Archives 5 years after cutoff.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

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

SYSTEM MANAGER(S):

Deputy Secretary, 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.

HISTORY:

89 FR 58780 (July 19, 2024)

SYSTEM NAME AND NUMBER:

Transit Subsidy Benefits Program Records—NRC 26.

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

Facility, Logistics and Support Branch, Office of Administration, NRC, Two White Flint North, 11545 Rockville Pike, Rockville, Maryland.

SYSTEM MANAGER(S):

Chief, Facility, Logistics and Support 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 other types of 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 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) the NRC suspects or has confirmed that there has been a breach of the system of records, (2) the NRC has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the 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 electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Accessed by name and SmarTrip 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:

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.

HISTORY:

89 FR 58781 (July 19, 2024)

SYSTEM NAME AND NUMBER:

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

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

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

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:

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.

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 part 20 of title 10 of the *Code of Federal Regulations* (10 CFR) 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, 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 licensees 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 other types of 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) the NRC suspects or has confirmed that there has been a breach of the system of records, (2) the NRC has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the 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 PDF files, TIFF files, ADAMS document profiles, and ADAMS digital signature and concurrence data are retained under 2.19.14.a(4) and are cut off at the end of the fiscal year and destroyed 2 years after cutoff. Personnel monitoring reports and personnel overexposure reports of which only selected data are entered into REIRS, records are retained under 2.19.14.b(1). Cut off at end of fiscal year. Transfer to National Archives and Records

Administration (NARA) when 20 years old.

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, Office of Nuclear Reactor Regulation (NRR), Office of Nuclear Material Safety and Safeguards (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 keycard 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.

HISTORY:

89 FR 58782 (July 19, 2024)

SYSTEM NAME AND NUMBER:

Special Inquiry Records—NRC 33.

SECURITY CLASSIFICATION:

Classified and Unclassified

SYSTEM LOCATION:

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

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 facilities or involving nuclear materials, or allegations 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 other types of 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. A record from this system 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. A record from this system 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) the NRC suspects or has confirmed that there has been a breach of the system of records, (2) the NRC has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the 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. 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). Cut off files upon license termination following completion of decommissioning procedure. 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).

HISTORY:

89 FR 58786 (July 19, 2024)

SYSTEM NAME AND NUMBER:

Drug Testing Program Records—NRC 35.

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

Division of Facilities and Security, Office of Administration, NRC, Two White Flint North, 11545 Rockville Pike, 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:

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 substances, 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 other types of 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) the NRC suspects or has confirmed that there has been a breach of the system of records, (2) the NRC has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the 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)

HISTORY:

89 FR 58787 (July 19, 2024)

SYSTEM NAME AND NUMBER:

Employee Locator Records—NRC 36.

SECURITY CLASSIFICATION:

SYSTEM LOCATION:

Records are maintained in a Federal Risk and Authorization Management Program (FedRAMP)-authorized cloud environment hosted by Amazon Web Services (AWS) within U.S. regions. System infrastructure is located in AWS U.S. East and U.S. West regions. Supporting system administration and operational activities may occur at contractor facilities in Vienna, Virginia, and Pasadena, California.

SYSTEM MANAGER(S):

Branch Chief, Security Operations Branch, Cyber and Information Security Division, Office of the Chief Information Officer, U.S. Nuclear Regulatory Commission, 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 to provide a platform for the NRC to notify employees and contractors of important events such as office or building closures, weather-related events, or other emergencies requiring notification. The system also supports personnel accountability during emergencies by allowing employees and contractors to report their status in response to system notifications.

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, personal email 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; 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 other types of 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) the NRC suspects or has confirmed that there has been a breach of the system of records, (2) the NRC has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the 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. Customer/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.

Employee emergency contact information records are retained under the National Archives General Records Schedule 5.3 item 020. Destroy when superseded or obsolete, or upon separation or transfer of employee. These records are used to account for and maintain communication with personnel during emergencies, office dismissal, and closure situations.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Electronic records are protected by password controls and multi-factor authentication. Access to, and use of, these records is limited to authorized individuals whose official duties require such access. Administrative, technical, and physical safeguards are implemented to protect records from unauthorized access, use, or disclosure.

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.

HISTORY:

89 FR 58788 (July 19, 2024)

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.

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).

RECORD SOURCE CATEGORIES:

NRC employees, contractors, consultants, and licensees.

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

In addition to the other types of 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) the NRC suspects or has confirmed that there has been a breach of the system of records, (2) the NRC has

determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the 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 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. Freedom of Information Act (FOIA), Privacy Act (PA), 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 Mandatory Declassification Review 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.

Classified information nondisclosure agreements which are maintained separately from the individual's official personnel folder are retained under the National Archives and Records Administration's General Records Schedule 4.2 item 121. Destroy records when 50 years old.

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).

HISTORY:

89 FR 58789 (July 19, 2024)

SYSTEM NAME AND NUMBER:

Mailing Lists—NRC 38.

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

Facilities, Logistics and Support Branch, Division of Facilities and Security, Office

of Administration, NRC, 11545 Rockville Pike, Rockville, Maryland.

SYSTEM MANAGER(S):

Facilities, Logistics and Support Branch, Division of Facilities and Security, 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 other types of 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) the NRC suspects or has confirmed that there has been a breach of the system of records, (2) the NRC has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the 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 maintained on paper and 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.

HISTORY:

89 FR 58791 (July 19, 2024)

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, 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, 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) the NRC suspects or has confirmed that there has been a breach of the system of records, (2) the NRC has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the 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. Indexes to the personnel security case files are retained according to General Records Schedule 5.6 item 190 and destroyed when superseded or obsolete.

Insider threat inquiry records are retained according to General Records Schedule 5.6 item 220 and destroyed 25 years after close of inquiry, 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).

HISTORY:

89 FR 58792 (July 19, 2024)

SYSTEM NAME AND NUMBER:

Facility Security Access Control Records—NRC 40.

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

Division of Facilities and Security, Office of Administration, NRC, Two White Flint North, 11545 Rockville Pike, 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. 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 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, 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 other types of 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) the NRC suspects or has confirmed that there has been a breach of the system of records, (2) the NRC has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the 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, 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 (NARA) General Records Schedule (GRS) 5.6, Security Management Records establishes retention requirements for visitor processing records and related security indexes. Visitor processing records for areas requiring the highest level of security awareness, including spaces designated by the Interagency Security Committee (ISC) as Facility Security Level (FSL) V, are covered under GRS 5.6, item 110 and are temporary records authorized for destruction when 5 years old, unless a longer retention period is required for business use. Visitor processing records for all other facility security areas, including those designated by ISC as FSL I through IV, are covered under GRS 5.6, item 111 and are temporary records authorized for destruction when 2 years old, unless longer retention is required for business use. Indexes to personnel security case files are covered under GRS 5.6, item 190 and are temporary records authorized for destruction when superseded or obsolete. The NARA GRS 5.6, Security Management Records establishes retention requirements for routine facility security operations, credentialing records, and personnel security investigative documentation. Facility security management operations records are covered under GRS 5.6, item 090 and are temporary records authorized for destruction when 30 days old, unless longer retention is required for business use. Records associated with personal identification credentials and cards, including application and activation records, are covered under GRS 5.6, item 120 and are temporary records authorized for destruction 6 years after the end of an employee or contractor's tenure, unless a longer retention period is required for business use. Personal identification cards are covered under GRS 5.6, item 121 and are temporary records authorized for destruction after expiration, confiscation, or return. Personnel suitability and eligibility

investigative reports are covered under GRS 5.6, item 170 and are temporary records authorized for destruction in accordance with the investigating agency's instructions. Reports and records created by agencies conducting investigations under delegated investigative authority are covered under GRS 5.6, item 171 and are temporary records authorized for destruction in accordance with the applicable 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.

HISTORY:

89 FR 58793 (July 19, 2024)

SYSTEM NAME AND NUMBER:

Employee Fitness Center Records—NRC 44.

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

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

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 other types of 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) the NRC suspects or has confirmed that there has been a breach of the system of records, (2) the NRC has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the 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 retained according to the National Archives and Records Administration's General Records Schedule 2.7: Employee Health and Safety Records, item 080, Non-occupational health and wellness program records. 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. Electronic records are protected by screen saver. Access to electronic 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.

HISTORY:

89 FR 58798 (July 19, 2024)

SYSTEM NAME AND NUMBER:

Electronic Credentials for Personal Identity Verification–NRC 45.

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

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

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 Personal Identity Verification (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, e-mail 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) the NRC suspects or has confirmed that there has been a breach of the system of records, (2) the NRC has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the 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.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are retrievable by an individual's name, e-mail 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 6 years after the end of an employee or contractor's tenure, 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. 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.

HISTORY:

89 FR 58799 (July 19, 2024)

SYSTEM NAME AND NUMBER:

Health Emergency Records—NRC 46.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Headquarters, 11555 Rockville Pike, Rockville, Maryland. Records may be maintained at all locations at which the NRC, or contractors on behalf of the NRC,

operate or at which NRC operations are supported.

SYSTEM MANAGER(S):

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

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Workforce safety Federal requirements, which include: the Occupational Safety and Health Act of 1970; Executive Order 12196; and 5 U.S.C. 7902, “Safety programs.” Federal laws that authorize the NRC to create and maintain Federal records of agency activities, which include: 44 U.S.C. 3101; the Religious Freedom Restoration Act of 1993, 42 U.S.C. Chapter 21B; Title VII of the Civil Rights Act of 1964, as amended, 42 U.S.C. 2000e; and the Rehabilitation Act of 1973, as amended, 29 U.S.C. 701 *et seq.* Authorities addressing the federal government’s preparation for, and response to, public health threats, including the PREVENT Pandemics Act, 42 U.S.C. § 300hh-3; and Executive Order 13987, “Organizing and Mobilizing the United States Government to Provide a Unified and Effective Response to Combat COVID-19 and to Provide United States Leadership on Global Health and Security.”

PURPOSE(S) OF THE SYSTEM:

Maintaining records necessary and relevant to NRC activities responding to and mitigating high-consequence public health threats. Records may include, but are not limited to, those applicable health related records needed to understand the impact of an illness or disease on the NRC workforce or to assist the NRC in protecting its workforce from a declared public health emergency, pandemic, or other high-consequence public health threat, including records submitted by NRC personnel or by the lawful representative of such personnel.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

NRC employees.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records maintained in this system may include:

A. Full name, NRC employee ID number; telephone number, worksite, email address, supervisor's name, address and contact information.

C. Other information about the individual directly related to the disease or illness (*e.g.,* testing results/information, symptoms, treatments, source of exposure, or other applicable health related information).

D. Appointment scheduling information, including the date, time, and location of a scheduled appointment.

E. Medical screening information, including the individual's name, date of birth, age, category of employment, current medical status, related medical history, and any relevant medical history.

RECORD SOURCE CATEGORIES:

Records may be obtained from NRC employees or their representative who may provide relevant information on a suspected or confirmed disease or illness, or the prevention of such disease or illness, which is the subject of a high-consequence public health threat.

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

In addition to the other types of 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 herein if the disclosure is compatible with the purpose for which the record was collected under the following routine uses:

A. To appropriate medical facilities, or Federal, State, local, Tribal, territorial or foreign government agencies, to the extent permitted by law, for the purpose of protecting the vital interests of individual(s), including to assist the United States Government in responding to or mitigating high-consequence public health threats.

B. To determine eligibility for access to NRC buildings, NRC licensee facilities or sites, or other Federal facilities.

C. To provide licensees information needed for unescorted access or access to the licensee's facility or facilities.

D. Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate Federal, State, local, territorial, Tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.

E. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the NRC determines that the records are arguably relevant to its proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

F. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an NRC function related to this system of records.

G. A record on an employee from this system of records may be disclosed as a routine use to a Federal, State, local, territorial, Tribal, 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 that individual, letting a contract, or issuing a license, grant, or other benefit.

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

I. To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

J. To appropriate agencies, entities, and persons when (1) the NRC suspects or has confirmed that there has been a breach of the system of records, (2) the NRC has determined that as a result of the suspected or confirmed breach there is a risk of harm to an individual(s), the 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 the NRC's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

K. To another Federal agency or Federal entity, when the NRC determines that information from this system of records is 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.

L. To any agency, organization, or individual for the purpose of performing authorized audit or oversight operations of the NRC and meeting related reporting requirements.

M. To such recipients and under such circumstances and procedures as are

mandated by Federal statute or treaty.

N. 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 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.

O. To a Federal agency employee, expert, consultant, or contractor in performing a Federal duty for purposes of authorizing, arranging, and/or claiming reimbursement for official travel, including, but not limited to, traveler profile information.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

All records in this system of records are maintained and in compliance with applicable executive orders, statutes, and agency implementing recommendations. Electronic records are stored in databases. Paper records are maintained in a secure, access-controlled room, with access limited to authorized personnel.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records will be retrieved by any of the categories of records, including name, location, date of applicable health information, or work status.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

To the extent applicable, to ensure compliance with Americans with Disabilities Act, the Rehabilitation Act, and the Genetic Information Nondiscrimination Act of 2008, medical information must be “maintained on separate forms and in separate medical files and be treated as a confidential medical record.” 42 U.S.C. 12112(d)(3)(B); 42 U.S.C. sec 2000ff-5(a); 29 CFR 1630.14(b)(1), (c)(1),(d)(4)(i); and 29 CFR 1635.9(a). This means that medical information and documents must be stored separately from other personnel records. As such, the NRC must keep medical records for at least 1

year from creation date (29 CFR 1602.14). Further, records compiled under this system of records notice will be maintained in accordance with the National Archives and Records Administration General Records Schedule (GRS) 2.7, Employee Health and Safety Records, Items 010, 070, or 080 to the extent applicable.

GRS 2.7 item 010 (DAA-GRS-2017-0010-0001)—Clinic scheduling records. Temporary. Destroy when 3 years old, but longer retention is authorized if needed for business use.

GRS 2.7 item 070 (DAA-GRS-2017-0010-0012)—Non-occupational individual case files. Temporary. Destroy 10 years after the most recent encounter, but longer retention is authorized if needed for business use.

GRS 2.7 item 080 (DAA-GRS-2017-0010-0013)—Non-occupational health and wellness program records. Temporary. Destroy 3 years after the project/activity/or transaction is completed or superseded, but longer retention is authorized if needed for business use.

GRS 2.7 item 063 (DAA-GRS-2021-0003-0001)—Vaccination attestations and proof of vaccination records. Federal employees and contractors. Temporary. Destroy when 3 years old.

GRS 2.7 item 064 (DAA-GRS-2021-0003-0002)—Vaccination attestations and proof of vaccination records. Visitors. Temporary. Destroy when 30 days old.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

The NRC safeguards records in this system according to applicable rules and policies, including all applicable NRC automated systems security and access policies. The NRC has imposed controls to minimize the risk of compromising the information that is being stored. Users of individual computers can only gain access to the data by valid user identification and password. Paper records are maintained in a secure, access-

controlled room, with access limited to authorized 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 Officer or Privacy Act Officer, Office of the Chief Information Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, and comply with procedures contained in NRC's Privacy Act regulations, 10 CFR part 9.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

HISTORY:

89 FR 58800 (July 19, 2024)

[FR Doc. 2026-20438 Filed: 10/5/2026 8:45 am; Publication Date: 10/6/2026]