

**SYSTEM NAME AND NUMBER:**

Personnel Security Files and Associated Records—NRC 39.

**SECURITY CLASSIFICATION:**

Unclassified

**SYSTEM LOCATION:**

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

**SYSTEM MANAGER(S):**

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

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

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

**PURPOSE(S) OF THE SYSTEM:**

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

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

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

## **CATEGORIES OF RECORDS IN THE SYSTEM:**

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

## **RECORD SOURCE CATEGORIES:**

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

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

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

- a. To determine clearance or access authorization eligibility;
- b. To determine eligibility for access to NRC buildings or access to Federal automated

information systems or data;

c. To certify clearance or access authorization;

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

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

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

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

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

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

j. A record from this system of records may be disclosed as a routine use to a Congressional office from the record of an individual in response to an inquiry from the

Congressional office made at the request of that individual;

k. A record from this system of records may be disclosed as a routine use to NRC-paid experts or consultants, and those under contract with the NRC on a “need-to-know” basis for a purpose within the scope of the pertinent NRC task. This access will be granted to an NRC contractor or employee of such contractor by a system manager only after satisfactory justification has been provided to the system manager;

l. A record from this system of records may be disclosed as a routine use to appropriate agencies, entities, and persons when (1) NRC suspects or has confirmed that there has been a breach of the system of records, (2) NRC has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, NRC (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with NRC efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm; and

m. A record from this system of records may be disclosed as a routine use to another Federal agency or Federal entity, when the NRC determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

**POLICIES AND PRACTICES FOR STORAGE OF RECORDS:**

Records maintained on paper, tapes, and electronic media.

**POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:**

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

## **POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:**

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