SYSTEM NAME AND NUMBER:

Information Security Files and Associated Records—NRC 37.

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

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

SYSTEM MANAGER(S):

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

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

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

PURPOSE(S) OF THE SYSTEM:

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

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

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

CATEGORIES OF RECORDS IN THE SYSTEM:

These records include information regarding:

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

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

RECORD SOURCE CATEGORIES:

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

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

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

a. To prepare statistical reports for the Information Security Oversight Office;

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

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

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

e. A record from this system of records may be disclosed as a routine use in the course of discovery; in presenting evidence to a court, magistrate, administrative tribunal, or grand jury

or pursuant to a qualifying order from any of those; in alternative dispute resolution proceedings, such as arbitration or mediation; or in the course of settlement negotiations;

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

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

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

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

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are maintained on paper in file folders and on electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Accessed by name and/or assigned number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

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

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

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

alarmed vaults cleared for open storage of TOP SECRET information.

CONTESTING RECORD PROCEDURE:

Same as “Notification procedures.”

RECORD ACCESS PROCEDURE:

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

NOTIFICATION PROCEDURE:

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

EXEMPTIONS CLAIMED FOR THE SYSTEM:

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