SYSTEM NAME AND NUMBER:

Employee Locator Records—NRC 36.

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

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

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

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

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

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

SYSTEM MANAGER(S):

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

Administration, NRC, Washington, DC 20555-0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

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

PURPOSE(S) OF THE SYSTEM:

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

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

NRC employees and contractors.

CATEGORIES OF RECORDS IN THE SYSTEM:

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

RECORD SOURCE CATEGORIES:

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

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

In addition to the 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) NRC suspects or has confirmed that there has been a breach of the system of records, (2) NRC has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, NRC (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with NRC efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm; and

h. A record from this system of records may be disclosed as a routine use to another Federal agency or Federal entity, when the NRC determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to

individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Information is accessed by name.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

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

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

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

RECORD ACCESS PROCEDURES:

Same as "Notification procedures."

CONTESTING RECORD PROCEDURES:

Same as “Notification procedures.”

NOTIFICATION PROCEDURES:

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

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.