SYSTEM NAME AND NUMBER:

Facility Security Access Control Records—NRC 40.

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

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

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

SYSTEM MANAGER(S):

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

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

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

PURPOSE(S) OF THE SYSTEM:

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

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

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

CATEGORIES OF RECORDS IN THE SYSTEM:

The system includes information regarding: (1) NRC personal identification badges issued for continued access to NRC-controlled space; and (2) records regarding visitors to NRC. The records include, but are not limited to, an individual’s name, social security number, electronic image, badge number, citizenship, employer, purpose of visit, person visited, date

and time of visit, and other information contained on Government issued credentials.

RECORD SOURCE CATEGORIES:

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

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

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

k. A record from this system of records may be disclosed as a routine use to another Federal agency or Federal entity, when the NRC determines that information from this system of

records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are maintained on paper and electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

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

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

The National Archives and Records Administration's General Records Schedule 5.6 includes Security Records. Visitor processing records in areas requiring highest level security awareness, including areas designated by the interagency Security Committee as Facility Security Level V, are retained according to General Records Schedule 5.6, item 110. Destroy when 5 years old, but longer retention is authorized if required for business use. Visitor processing records in facility security areas not requiring highest level security awareness, including areas designated by the interagency Security Committee as Facility Security Levels I through IV, are retained under General Records Schedule 5.6, item 111. Destroy when 2 years old, but longer retention is authorized if required for business use. Indexes to personnel security case files are retained under General Records Schedule 5.6, item 190. Destroy when superseded or obsolete. Records of routine security operations are retained under General Records Schedule 5.6, item 090. Destroy when 30 days old, but longer retention is authorized if required for business use. Personal identification credentials and cards, including application and activation records, are retained according to General Records Schedule 5.6, item 120. Destroy 6 years after the end of an employee or contractor's tenure, but longer retention is

authorized if required for business use. Personal identification cards are retained according to General Records Schedule 5.6 item 121 and destroyed after expiration, confiscation, or return. Personnel suitability and eligibility investigative reports are retained according to General Records Schedule 5.6, item 170. Destroy in accordance with the investigating agency instruction. Reports and records created by agencies conducting investigations under delegated investigative authority are retained according to General Records Schedule 5.6, item 171. Destroy in accordance with delegated authority agreement or memorandum of understanding.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

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

RECORD ACCESS PROCEDURES:

Same as "Notification procedures."

CONTESTING RECORD PROCEDURES:

Same as "Notification procedures."

NOTIFICATION PROCEDURES:

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

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.