SYSTEM NAME AND NUMBER:

Electronic Credentials for Personal Identity Verification–NRC 45.

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

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

Duplicate system–Duplicate systems may exist, in whole or in part, at the locations listed in Addendum I, Part 2.

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 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) 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

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 or on paper.

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 mandatory and optional data elements housed in the agency identity management system and printed on the identification card 6 years after terminating an employee or contractor's employment, 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. Hard copy documents are maintained in locking file cabinets. 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.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Disclosure of system records to consumer reporting systems is not permitted.