REQUEST FOR RECORDS DISPOSITION AUTHORITY

(See Instructions on reverse)

TO NATIONAL ARCHIVES and RECORDS ADMINISTRATION (NIR)
WASHINGTON, DC 20408

1 FROM (Agency or establishment)
U.S. Nuclear Regulatory Commission

2 MAJOR SUBDIVISION
Office of Information Services

3 MINOR SUBDIVISION
Infrastructure & Computer Operations Division

4 NAME OF PERSON WITH WHOM TO CONFER **Mary L. Haynes** Mary L. Haynes	5 TELEPHONE **(301) 415-6625**

LEAVE BLANK (NARA use only)

JOB NUMBER N1-431-09-3

DATE RECEIVED 9/16/09

NOTIFICATION TO AGENCY

In accordance with the provisions of 44 U S C 3303a the disposition request, including amendments, is approved except for items that may be marked "disposition not approved" or "withdrawn" in column 10

DATE 7/29/10	ARCHIVIST OF THE UNITED STATES WITHDRAWN

6 AGENCY CERTIFICATION
I hereby certify that I am authorized to act for this agency in matters pertaining to the disposition of its records and that the records proposed for disposal on the attached 2 page(s) are not now needed for the business of this agency or will not be needed after the retention periods specified; and that written concurrence from the General Accounting Office, under the provisions of Title 8 of the GAO Manual for Guidance of Federal Agencies,

☑ is not required; □ is attached; or □ has been requested

DATE 8/31/09	SIGNATURE OF AGENCY REPRESENTATIVE **Deborah H. Armentrout, CRM**	TITLE **NRC Records Officer**

7 ITEM NO	8 DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9 GRS OR SUPERSEDED JOB CITATION	10 ACTION TAKEN (NARA USE ONLY)
	TITLE: Public Key Infrastructure (PKI)		WITHDRAWN 7/29/10

for 8/24/09
PMDA Director, Sharon Stewart **Date**

8/30/09
Office of General Counsel **Date**

This form was designed using InForms

Public Key Infrastructure (PKI) enables users of an unsecure public network, such as the Internet, to securely and privately access or exchange data and payments through the use of a public and private cryptographic key pair authenticated through a trusted authority It is one of the principal technologies used to conduct business electronically. NRC's Certification Authority (CA) conforms with the Federal Bridge Certification Authority (FBCA) X 509 Certificate Policy which established four minimum retention levels or classes of assurance that reflect the agency's accepted levels of security risk for unauthorized access to or loss of the information record that the PKI protects and/or accesses under the CA This schedule covers CAs issued for unique Administrative and other administrative records, as well as PKI transaction-specific records that are part of the PKI trust documentation set used to support the integrity of the transaction. PKI unique administrative records establish or support authentication by tying the user to a valid electronic credential such as the CA or Certification Revocation List used to validate the signer's certificate, subscriber agreement and certificate validation responses.

WITHDRAWN

1. **Certification Authority (CA).**

These records consist of CA archive records that include system initialization records covering CA accreditation, certificate practice statements, and any contractual agreements to which the CA is bound Also consists of system configuration records and CA operational records, such as modifications or updates; certificate requests and revocation requests, subscriber identity authentication, as required; documentation of receipt and acceptance of certificates, documentation of receipt of tokens; all certificates and certificate revocation lists (CRL) or any other revocation information as issued or published; security audit records and data; additional data or applications sufficient to verify archive contents, and all work-related communications to or from the Program Management Authority, other Certification Management Authority and/or compliance auditors.

a. **Rudimentary CA records (Class 1).** These low-level CA operation records relate to system initialization equipment whose records include validation certificates that consist of the E-mail addresses of the individuals to whom the certificates are issued

Disposition: **Temporary.** Destroy/delete 1 year after the record to which the digital signature is applicable is no longer needed, whichever is sooner.

b. **Basic Assurance CA records (Class 2).** These records relate to system initialization equipment or CA operation and are usually retained for audit or transactional purposes.

WITHDRAWN

Disposition: **Temporary.** Destroy/delete after 7 years 6 months or when no longer needed for current business whichever is later

c. **Medium Assurance CA records (Class 3).** These records relate to system initialization equipment or CA operation and include all policies

WITHDRAWN

Disposition: **Temporary.** Destroy/delete when 10 years 6 months, or when no longer needed for current business whichever is later

d. High Assurance CA records (Class 4) These records relate to system initialization equipment or CA operation.

Disposition. **Temporary.** Destroy/delete when 20 years 6 months old, based on the maximum retention period of the CA, or when no longer needed for current business, whichever is later

2. PKI Administrative records. These administrative records attest to the reliability of the PKI transaction process The records include general operational procedures, agency policies, and legal counsel opinions, client/browser and server set up and configuration records, and application or system testing and validation records

Disposition **Temporary.** Destroy or delete based on the maximum retention period of the corresponding CA, and after the informational record on which the PKI is designed to protect or access is destroyed in accordance with an approved schedule or when no longer needed for business, whichever is later

WITHDRAWN

3. PKI Transaction-specific records. These are program records that relate to transaction specific records generated using PKI digital signature technology The records are embedded or referenced within the transaction stream and may be appended to the transaction content or information records.

a Records to which the CA relates that have a temporary disposition.

Disposition: **Temporary** Destroy/delete when 7 years 6 months to 20 years 6 months based on the maximum retention period of the corresponding CA and after the information record that the PKI is designed to protect or access is destroyed in accordance with an approved schedule, or when no longer needed for current business

b. Records to which the CA relates that have a permanent disposition.

Disposition: **Permanent.** Transfer the records to NARA in accordance with the regulations found 36 CFR § 1228.270 or other applicable NARA standards when the permanent records to which they relate are transferred

WITHDRAWN