ML040920340

U.S. Nuclear Regulatory Commission

Privacy Impact Assessment

General system/application (system) information (See definitions at end of document)

1. Person completing this form:

Name	Title	Phone #	E-mail	Office
Christine Hite	Fees Systems Analyst	(301) 415-8191	cwh1@nrc.gov	OCFO

2. System owner:

Name	Title	Phone #	E-mail	Office
Robert Carlson	Team Chief	(301) 415-8165	rdc@nrc.gov	OCFO

3. Person performing privacy review:

Name	Title	Phone #	E-mail	Office
Sandra Northern	Privacy Program Officer	(301) 415-6879	ssn@nrc.gov	OCIO

4. What is the name of this system? UPI # 429-00-01-01-01-2020-00-307-117

Fees Systems

5. Briefly describe the purpose of this system (support of what agency function)?

The Fees Systems produce management reports and invoices for fee billable services performed by the Nuclear Regulatory Commission (NRC). The type of expenditure associated with this project

is categorized as a "Legacy System Application" and it is in the Evaluate Phase of the Capital Planning and Investment Control (CPIC) process.

The Nuclear Regulatory Commission (NRC) is required to recover a major portion of its annual budget. In order to implement this requirement, the NRC assesses fees in compliance with the Omnibus Budget Reconciliation Act of 1990 (OBRA-90), as amended, and the Independent Offices Appropriation Act of 1952 (IOAA). Fees are recovered as established in 10 CFR Part 170 and 10 CFR Part 171 of the Commission's regulations.

The Office of the Chief Financial Officer/Division of Accounting and Finance/License Fees and Accounts Receivable Branch (OCFO/DAF/LFARB) administers some components of the License Fee Management Program through use of automated processes. The Fees Systems are comprised of a number of sub-application systems. The applications share data from various sources throughout the Agency. The primary function of these applications is to generate invoices to licensees for annual fees and fees for various services which include new licensing approvals, licensing amendments, topical reports, and inspections. Additional functionality includes the tracking of new small materials licensing application fee payments.

6. **Does this system contain any personal information (name, social security number, date of birth, home address, etc) about individuals?**

   Yes X No____

   If no, stop here and return this form to John Sullivan, OCIO, jas2@nrc.gov.

   If yes, please complete remainder of form.

Data in the System

1. **What type of information is being maintained in the system (financial, medical, training, personnel, etc)?**

NRC employees' initials and names are used, as well as names and addresses of licensees. Licensees include over 50 categories of persons required to be licensed as well as, where applicable, applicants for facilities, materials, import and export licenses, holders of certificates of compliance, registrations, quality assurance program approvals and government agencies licensed by the NRC.

2. **Source of the information in this system.**

a. Is data being collected from the subject individual? If yes, what type(s) of data is being collected?

The data is not collected from the subject individual.

b. Is data on this individual being collected from other NRC files and databases for this system? If yes, identify the files and databases?

The data is collected from other NRC files and databases that include the following:

- Human Resource Management System (HRMS) – time and labor
- Reactor Program System (RPS) – Staff, TAC and Facility tables
- Inspection Reports Tracking System (IRTS) – inspection reports
- License Tracking System (LTS) - Licensee name and address
- Transportation Approval Package Information System (TAPIS) - Licensee name and address
- National Sealed Source and Device Registry System (NSS&DRS) - Licensee name and address
- Technical Assistance Program Support System (TAPSS) – contract costs
- Technical Assistance Program Support System/NMSS (TAPNM) – contract costs

c. Is data on this individual being collected from source(s) other than the subject individual and NRC records? If yes, what is the source(s) and what type(s) of data is being collected?

Billing addresses are sometimes provided directly from the licensees.

d. How will data collected from source(s) other than the subject individual or NRC records be verified as current, accurate, and complete?

Licensees are required to provide correct information for new and changed addresses.

Are the data elements described in detail and documented? If yes, what is the name of the document?

The data elements are described in detail and fully documented in User Guides and As-Built System Documents.

Attributes of the Data

Is the use of the data both relevant and necessary for the purpose for which the system is designed?

Yes.

Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

a. How will aggregated data be maintained, filed, utilized?

Data is stored and maintained in DB2 and dBase databases.

b. How will aggregated data be validated for relevance and accuracy?

Certification and management procedures are in place to validate relevance and accuracy.

If data is consolidated, what controls protect it from unauthorized access/use?

The Fees Systems authorization/access control functionality is provided through several different functional levels. These levels are integrated into the process depending on which function is being performed. User identification and authentication are implemented via the mainframe security features of IMB's Resource Access Control Facility (RACF) and within the environment via Novell LAN Manager security features. Administrative, physical, and personnel security requirements are specified and documented. Additional technical security specifications are also built into the systems.

How will the data be retrieved?

a. Can it be retrieved by personal identifier? If yes, explain.

Staff names are retrieved from a Staff table via unique initials that are assigned to each NRC employee. Licensee names and addresses will be retrieved from the various source tables via License Number, TAC Number, Registration Number, and Docket Number.

What type(s) of report(s) can be produced from this system?

Many reports that include information pertaining to staff effort and licensing actions on fee billable activities are produced. Various types of invoices are also produced.

a. What are the reports used for?

Reports are used to verify fee billable effort and to provide financial statistics for management. Invoices are sent to licensees for fee collection.

b. Who has access to these reports?

NRC Program Offices such as the Office of the Chief Financial Officer (OCFO), Office of Nuclear Material Safety and Safeguards (NMSS), the Office of Nuclear Reactor Regulation (NRR), Regional Offices, contractors and the general public.

<u>Maintenance of Administrative Controls</u>

1. What is the retention period of the data in this system? [If preparer does not know the answers to a. - c.,, they should so state and OCIO will fill in]

a. What are the procedures for disposition of the data at the end of the retention period?

Unless otherwise specified in NARA guidelines, residual sensitive data is placed in "burn bags" for periodic collection by NRC security employees for destruction. The material is then destroyed by shredding.

b. How long will produced reports be maintained?

Unless otherwise specified in NARA regulations and/or NRC Management Directive 4.6, data are required to be retained for 6 years and 3 months in accordance with General Records Schedule (GRS) 6-1.a(a). Electronic records from the fees systems are required to be retained until the data is no longer needed in accordance with the NRC Comprehensive Description Schedule (NRCS) 2-10.3 (NUREG-0910)(b). Program Offices retain certified hardcopy cost data, used to determine fees, for 6 years and 3 months in accordance with NRCS 1-1.8(a). Input records used to update staffing reporting systems are retained until the information has been converted to an electronic medium and verified, or until no longer needed to support the reconstruction of or serve as the backup of the master file, whichever is later, in accordance with GRS 20-2.a(b).

c. **Where are the reports stored?**

Sensitive data is protected in secured operating areas and procedures for clearing sensitive data from plain view at the close of each workday are in effect. Approved file cabinets are used for storage.

d. **Where are the procedures documented?**

Procedures are documented in Branch internal operating procedures.

2. **Will this system provide the capability to identify, locate and monitor individuals? If yes, explain.**

Under the Freedom of Information Act (FOIA), general licensees will be permitted to review data utilized by the Fees Systems Replacement, which pertain to them. The names, addresses and fee schedules for companies that are recorded in the system may be released to the public upon request.

a. **What controls will be used to prevent unauthorized monitoring?**

Access is monitored through various methods including user identification and authentication. Audit trails are maintained.

3. **Under which Privacy Act system of records (SOR) notice does this system operate (link to list of SOR available on NRC Internal Home page)? Provide number and name. [If preparer unable to determine, they should call Sandra Northern, 415-6879].**

The Fees Systems operate as noted in the Federal Register of October 15, 2002 "Part III, Nuclear Regulatory Commission, Privacy Act of 1974; Republication of Systems of Records Notices; Notice". The system number is NRC-32: Office of the Chief Financial Officer Financial Transactions and Debt Collection Management Records.

a. **If the system is being modified, will the SOR notice require amendment or revision? Explain.**

Modification of the Fees Systems does not require amendment or revision of the SOR notice.

<u>Access to the Data</u>

1. **Who will have access to the data in the system (users, managers, system administrators, developers, other)?**

   Authorized NRC staff have various, appropriate levels of access to the data and NRC licensees have access to printed output only, i.e., invoices.

2. **Are criteria, procedures, controls, and responsibilities regarding access documented?**

Yes.

3. **Will users have access to all data in the system or will users access be restricted? Explain.**

   Access is restricted at various levels and different components are controlled individually.

4. **What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?**

   Access is monitored and audit trails are maintained.

5. **Do other systems share data or have access to data in this system?**

   Yes.

6. **Will other agencies share data or have access to data in this system (Federal, State, Local, other)? Explain.**

   Data pertaining to billing transactions and licensee names/addresses are sent electronically to the U.S. Department of Treasury.

7. **Were Privacy Act clauses cited and other regulatory measures addressed in contracts with contractors having access to this system?**

Privacy Act clauses were cited and other regulatory measures were addressed in contracts with contractors that have access to the Fees Systems.

Return completed Privacy Act Assessment to John Sullivan, OCIO, jas2@nrc.gov.

DEFINITIONS

Personal Information is information about an identifiable individual that may include but not be limited to:

- race, national or ethnic origin, religion, age, marital or family status
- education, medical, psychiatric, psychological, criminal, financial, or employment history
- any identification number, symbol, or other particular assigned to an individual
- name, address, telephone number, fingerprints, blood type, or DNA

Aggregation of data is the taking of various data elements and then turning them into a composite of all the data to form another type of data such as tables or data arrays, or collecting data into a single database.

Consolidation means combining data from more than one source into one system, application, or process. Existing controls for the individual parts should remain or be strengthened to ensure no inappropriate access by unauthorized individuals. However, since individual pieces of data lose their identity, existing controls may actually be diminished - e.g: a summary census report may not point at the individual respondent but rather at a class of respondents, which makes it less personal.