

U.S. Nuclear Regulatory Commission Privacy Impact Assessment

Instructions: **Section A, B, C, and D must be completed for all systems. Section E must be completed if yes is the answer to Section B, questions 1 and 2.**

Date: 03/23/2006 Re-submission

A. GENERAL SYSTEM/APPLICATION INFORMATION

(See definitions at end of document)

1. Person completing this form:

| Name | Title | Phone No. | Office |
|-----------------|-------------------|--------------|--------|
| Kathleen Brosky | Senior Accountant | 301-415-6076 | OCFO |

2. System owner:

| Name | Title | Phone No. | Office |
|---------------|-------------------------|--------------|--------|
| Jesse Funches | Chief Financial Officer | 301-415-7322 | OCFO |

3. What is the name of this system?

Cost Accounting System (CAS)

4. Briefly describe the purpose of this system. What agency function does it support?

CAS is used to support one of the financial statements, and provides full cost data.

5. Note below whether this Privacy Impact Assessment supports a proposed new system or a proposed modification to an existing system.

_____ New System X Modify Existing System

B. PRIVACY ACT APPLICABILITY

1. Does this system collect, maintain, or disseminate personal information in

identifiable form (e.g., name, social security number, date of birth, home address, etc.) about individuals ?

Yes ☒ No ☐ Employee ID and name only.

2. If yes, will the data be retrieved by an individual's name or other personal identifier (e.g., social security number, badge number, etc.)?

Yes ☒ No ☐ Employee ID and name only.

If you answer yes to questions 1 and 2, complete Section E.

C. INFORMATION COLLECTION APPLICABILITY

1. Will the personal data be collected from or maintained by persons who are not Federal employees?

Yes ☐ No ☒

2. Will the data be collected from Federal contractors?

Yes ☐ No ☒

3. If the answer is yes to either question 1 or 2, will the data be collected from 10 or more persons during a calendar year?

Yes ☐ No ☐

4. If the answer is yes to question 3, is the information to be collected covered by an existing OMB clearance number? If yes, indicate the clearance number, 3150-__ __ __ __

D. RECORDS RETENTION AND DISPOSAL SCHEDULE APPLICABILITY

Does this system already have a NARA-approved records disposition schedule? (Reference NUREG-0910, "NRC Comprehensive Records Disposition Schedule," or contact your office Records Liaison Officer or Jeff Bartlett, OIS.)

Yes ☐ No ☒

If yes, list the records schedule number _____

| |
|---|
| <i>Complete Section E only if the answers to Section B, questions 1 and 2 are Yes.</i> |
|---|

E. SYSTEM DATA INFORMATION

1. *Type of information maintained in the system*

- a. Describe the information to be maintained in the system (e.g., financial, medical, training, personnel.) Give a detailed description of the data.

CAS data includes financial data such as NRC employees' names, employees' ID number, labor hours, organizational units, and salary and benefit costs.

2. *Source of the data in this system*

- a. Are data being collected from the subject individual? If yes, what types of data are being collected?

No.

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

Yes. The data is extracted through interface from the NRC's Human Resources Management System (HRMS), the NRC's Reactor Program System (RPS), and the NRC's Federal Financial System (FFS). Employee hours and dollars are validated against reports from the HRMS at the aggregated level each pay period. FFS is validated against FFS reports.

- c. Are data on this individual being collected from a source or sources other than the subject individual and NRC records? If yes, what is the source and what type of data is being collected?

No.

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

NA

3. *Attributes of the data*

- a. Are the *data elements* described in detail and documented? If yes, what is the name of the document? Where is it located?

Yes. A CAS User Manual and System Documentation is located with the system administrator. Formal data dictionaries describing the data elements in detail are contained within the system data dictionaries for each source system (HRMS, FFS, and the RPS).

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

Yes.

- c. Will the system derive (i.e., create) new data or create previously unavailable data about an individual through aggregation from the information collected?

Yes.

- (1) How will aggregated data be maintained, filed, and utilized?

The CAS contains a labor distribution files and model that combines an individuals hours worked, along with their salaries and benefits for each pay period. The CAS assigns the salaries and benefits on a pro-rata share to the hours the employee worked during each pay period. This data is maintained in detail databases, file and reports and used for financial statement reporting.

- (2) How will aggregated data be validated for relevance and accuracy?

Employee hours and dollars are validated against reports from the HRMS at the aggregated level each pay period. Furthermore, audit detail databases are created; and, CA personnel and auditors perform detail tests on samples individuals to ensure that the LDM is accurate and functioning as designed.

4. If data are consolidated, what *controls* protect it from unauthorized access, use, or modification?

Consolidated data is protected by authorized user access to the CAS server and application. Log-in credentials are validated at both the LAN level and within CAS. CAS verifies the accuracy of the password entered as well as matches the password used to access the CAS with the password used to log into the workstation connected to the LAN. Using Novell's eDirectory API, CAS validates a user's credentials utilizing the user's authenticated identity that is established during the user's login to the NRC network. Validation is accomplished by passing the user's credentials to a local Novell DLL function, which in turns performs the validation. For authorization, CAS utilizes a role-based access model, and stores that accessibility information in the CAS database. Specialized CAS software is located only on authorized users workstations.

5. How will the data be *retrieved* from the system?

- a. Can it be retrieved by personal identifier? X Yes No

If yes, explain.

The data can be retrieved by authorized CA users by employee name and by employee ID.

- b. Is a password or data description required? X Yes No
If yes, explain.

Passwords are used to gain access to the CAS application. . Log-in credentials are validated at both the LAN level and within CAS. CAS verifies the accuracy of the password entered as well as matches the password used to access the CAS with the password used to log into the workstation connected to the LAN. Using Novell's eDirectory API, CAS validates a user's credentials utilizing the user's authenticated identity that is established during the user's login to the NRC network. Validation is accomplished by passing the user's credentials to a local Novell DLL function, which in turns performs the validation. For authorization, CAS utilizes a role-based access model, and stores that accessibility information in the CAS database.

6. Describe the report or reports that can be produced from this system.

- a. What reports are produced from the system?

Reports generated from the system provide costs by office, resource, program, planned activity, activity code, employee, on a pay period, monthly, and year-to-date basis. CAS does not produce any external reports; however the system produces reports used to develop a portion of the Financial Statement of Net Cost.

- b. What are the reports used for?

The reports are used to develop a portion of the Financial Statement of Net Cost. Some reports are used to monitor budget execution; however, FFS reports are the primary source of budget execution data.

- c. Who has access to these reports?

Hard copy reports are distributed to NRC office directors, accountants, budget analysts, functional managers, and financial auditors. Softcopy reports are sent via email to NRC regional offices. Soft copies of databases, reports and files are provided to the financial auditors. Reports are generated by CA personnel only and retained as PDF files.

7. *Records retention*

- a. What are the record types contained in this system and the medium on which they reside? (Examples: type - program records, medium -

electronic; type - database, medium - electronic; type - system documentation, medium - paper.)

Type is database and the medium is electronic.

- b. What is the NARA-authorized retention period for each records series in this system?

3 years

- c. If unscheduled, what are your retention requirements for each records series in this system?

Hardcopy reports are retained for one year. Electronic medium is retained indefinitely.

- d. What are the procedures for disposing of the data at the end of the retention period (specifically address paper copy, magnetic, or other forms of media)?

Paper copy reports that do not contain Privacy Act sensitive material (i.e., of public record) are disposed of through the NRC's paper recycling efforts. Privacy Act sensitive material is disposed of in accordance with NARA regulations. (As a precaution all paper copy reports are disposed of in the Classified and Sensitive Unclassified Waste containers).

- e. How long will produced reports be maintained?

Hard copy reports are retained for 1 year and available via backup within the NARA guidelines. Electronic medium is retained indefinitely. Both electronic reports and backup are controlled by user access controls and availability by workstation.

- f. Where are the reports stored?

Hardcopies are stored within the Office of the Chief Financial Officer and softcopies are stored on the CA production server.

- g. Where are the procedures for maintaining the data/reports documented?

Documented in the CAS documentation is located with the system administrator and on the cost accounting production server.

- h. How will unused or unwanted reports be disposed of?

Paper copy reports that do not contain Privacy Act sensitive material (i.e., of public record) are disposed of through the NRC's paper recycling efforts. Privacy Act sensitive material is disposed of in accordance with

NARA regulations. (As a precaution all paper copy reports are disposed of in the Classified and Sensitive Unclassified Waste containers).

8. Capability to *monitor individuals*

a. Will this system provide the capability to identify, locate, and monitor (e.g., track, surveillance) individuals? ___ Yes X No.
If yes, explain.

b. What controls will be used to prevent unauthorized monitoring?

NA

9. Coverage Under Existing *Privacy Act System of Records*

a. Under which Privacy Act System of Records (SOR) notice does this system operate (link to list of SOR available on NRC Internal Home Page)?

NRC-21, "Payroll Accounting Records"

b. If the Privacy Act System of Records is being modified, will the SOR notice require amendment or revision? ___ Yes X No.
If yes, explain.

10. Access to the Data

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

Authorized CA personnel only.

b. Are criteria, procedures, controls, and responsibilities regarding access documented? If so, where?

Yes. The CAS documentation is located with the system administrator and copies are located on the CA server.

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

User access to data is restricted by the CA user ID. The system will allow varying degrees of access by function.

d. What controls are or will be in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?

The CAS is not an original point of entry for any data. The system simply extracts data through interfaces from various systems. Users do not have the capability to alter data of official record. User access is limited by job function and a "need to know."

- e. Do other systems share data or have access to data in this system?
___ Yes X No. If yes, explain.
- f. Will other agencies share data or have access to data in this system
(Federal, State, local, other)? ___ Yes X No.
- g. Were Privacy Act clauses cited (or will be cited) and were other regulatory
measures addressed in contracts with contractors having access to this
system? X Yes ____ No. If yes, explain.

The CA contractor is on the same contract as the HRMS contractor and
the PA FAR clauses are referenced the contract.

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.

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL
(For Use by OIS Staff)

System Name: **Cost Accounting System (CAS)**

Submitting Office: **Office of the Chief Financial Officer (OCFO)**

A. PRIVACY ACT APPLICABILITY REVIEW

☐ Privacy Act is not applicable.

☒ Privacy Act is applicable. Currently covered under System of Records, NRC-21, "Payroll Accounting Records." No modification to the system notice is required.

☐ Privacy Act is applicable. Creates a new system of records. FOIA/PA Team will take the lead to prepare the system notice.

☐ Privacy Act is applicable. Currently covered under System of Records, NRC _____. Modification to the system notice is required. FOIA/PA Team will take the lead to prepare the following changes:

Comments:

The answer to E.1.a. was revised to include employee ID number per conversation with Kathleen Brosky. The last Privacy Act applicability review performed on 12/13/2005.

| Reviewer's Name | Title | Date |
|--------------------|-------------------------|----------------|
| Sandra S. Northern | Privacy Program Officer | March 28, 2006 |

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

☒ No OMB clearance is needed.

☐ OMB clearance is needed.

☐ Currently has OMB Clearance.

Comments:

Based on the information provided for this system, there is no data collected from the public. Therefore, no OMB clearance is needed.

| Reviewer's Name | Title | Date |
|------------------------|-------------|----------------|
| Christopher J. Colburn | Team Leader | March 28, 2006 |

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

- ☒ Additional information is needed to complete assessment.
- ☒ Needs to be scheduled.
- ☐ Existing records retention and disposition schedule covers the system - no modifications needed.
- ☐ Records retention and disposition schedule must be modified to reflect the following:

Comments:

NRC Form 616 and 637 were not provided with this re-submission of the Privacy Impact Assessment. As stated in the previous PIA review of this system, it appears that the system contains official records, but does not have a NARA approved retention period established. Further dialog and records management review is required to determine appropriate disposition for the system. However, further records management review does not preclude moving forward with the certification of this system.

| Reviewer's Name | Title | Date |
|-----------------|------------------------|-----------|
| Jeff Bartlett | Senior Records Analyst | 3/28/2006 |

D. BRANCH CHIEF REVIEW AND CONCURRENCE

- ☒ Does not constitute a Privacy Impact Assessment required by the E-Government Act of 2002
- ☐ Does constitute a Privacy Impact Assessment required by the E-Government Act of 2002 and requires approval of the Director, IRSD.

CONCUR IN REVIEW: /RA/ Date: **03/29/2006**

Brenda J. Shelton, Chief
Records and FOIA/Privacy Services Branch

E. DIVISION DIRECTOR APPROVAL OF PRIVACY IMPACT ASSESSMENT:

(Approval is only required when Yes is given to Section B, questions 1 and 2 and Section C, question 1. The system collects, maintains, or disseminates personal information in identifiable form about members of the public.)

John J. Linehan, Director, Information and Records Services Division

Date: / /

**TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS**

| | | |
|--|--|--------------------------------------|
| TO: (Sponsoring Office) Office of the Chief Financial Officer | Office Sponsor: Jesse Funches | |
| Reginald W. Mitchell, Director Business Process Improvement and Applications Division, Office of Information Services | Name of System: Cost Accounting System (CAS) | |
| Kathy L. Lyons-Burke, CISSP Senior IT Security Officer (SITSO)/ Chief Information Security Officer (CISO) Office of Information Services | Date Received: 03/24/2006 | Date Completed: 03/29/2006 |
| <p>Noted Application Development and System Security Issues:</p> <p>Currently covered under Privacy Act System of Records, NRC-21, "Payroll Accounting Records." No modification to the system notice is required.</p> <p>No information collection issues.</p> <p>Further dialog and records management review is required to determine appropriate disposition for the system. However, further records management review does not preclude moving forward with the certification of this system.</p> | | |
| Brenda J. Shelton, Chief Records and FOIA/Privacy Services Branch, OIS | Signature: /RA/ | Date: 03/29/2006 |