ADAMS ML061180261

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:

A. GENERAL SYSTEM/APPLICATION INFORMATION

(See definitions at end of document)

1. Person completing this form:

Name	Title	Phone No.	Office
Arthur Davis	Technical Project Manager	(301) 415-5780	OIS
Margie Dimig	Project Manager	(301) 415-5781	OIS

2. System owner:

Name	Title	Phone No.	Office
Reginald Mitchell	Director, Business Process Improvement and Applications Division	(301) 415-0387	OIS

3. What is the name of this system?

Case Management System (CMS). This system was previously identified as ICASES. There are three applications being replatformed that will reside under this umbrella title. The three applications are the Enforcement Action Tracking System (EATS), the Allegations Management System (AMS) and the Office of Investigations Management Information System (OIMIS).

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

The purpose of this effort is to replatform the Allegation Management System (AMS), Enforcement Action Tracking System (EATS), and Office of Investigation Management Information System (OIMIS) from a client/server environment into a Web environment in the 3-Tier architecture that will be accessed via a Web browser on the NRC Internal Web site. The design of these applications will allow data common to all 3 systems to be shared electronically. This common data was previously shared manually on a need to know basis to perform official duties. Each office needs to store and retrieve data to

perform their business functions in a timely manner. Presently, those systems are legacy applications and are very costly to maintain.

5. Does this Privacy Impact Assessment support a proposed new system or a proposed modification to an existing system.

__New System _✔__ Modify Existing Systems

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_____

OIMIS - Individuals and entities referred to in potential or actual investigations and matters of concern to the Office of Investigations.

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 ✔

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 X__ No ___

2. Will the data be collected from Federal contractors?

Yes ____ No _X__

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 _X__ 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.

No. 3150-0044

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 _____

Complete Section E only if the answers to Section B, questions 1 and 2 are Yes.

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.

   These systems contain sensitive allegation, enforcement action, and investigation data involving actual or alleged criminal and civil/regulatory violations. OIMIS may include witness and subject names and personal identifiers as well as personal background information with address and phone numbers. These systems will contain detailed information on current and completed allegations, enforcement actions, and investigations with pre-decisional information for enforcement actions.

2. *Source* of the data in this system

   a. Are data being collected from the subject individual?

   Yes - OIMIS

.

   If yes, what types of data are being collected?

   See E.1.a above

   b. Are data on this individual being collected from other NRC files and databases for this system?

   Yes, if applicable.

   If yes, identify the files and databases.

License files and the Reactor Program System (RPS).

c. Are data on this individual being collected from a source or sources other than the subject individual and NRC records?

Yes - OIMIS

If yes, what is the source and what type of data is being collected?

Criminal history - NCIC
Individual and business information

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

Through public records such as credit checks, property records, investment records, and Dun and Bradstreet Reports.

3. *Attributes* of the data

a. Are the *data elements* described in detail and documented?

Yes

If yes, what is the name of the document? Where is it located?

The documentation is stored in the Rational ClearCase VOB.
System Architecture Document
AS-Built Document
AMS Users Guide
EATS Users Guide
OIMIS Users Guide

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

Yes for all three systems.

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

No

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

N/A

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

N/A

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

   N/A

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

   a. Can it be retrieved by personal identifier? ___ Yes ✔ No.
   If yes, explain.

   b. Is a password or data description required? ✔ Yes ___ No.

   If yes, explain.

   Access is granted by the headquarters system administrator for each system..

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

   a. What reports are produced from the system?

   All systems - statistical, case summary

   b. What are the reports used for?

   All systems - Used to report various statistical data or summarized case data

   c. Who has access to these reports?

   All systems - Authorized staff members with a need to know.

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.)

   All systems: type - database, medium - electronic
   All systems: type - reports, medium - paper

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

   Unscheduled.

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

To be retained indefinitely, or until a NARA-authorized records schedule is implemented.

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)?

At this time data will not be destroyed.

e. How long will produced reports be maintained?

To be determined.

f. Where are the reports stored?

File cabinets.

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

System Requirement Specification
System Architecture Document
User Manual

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

Reports containing SUNSI information are disposed of through the Classified and Sensitive Unclassified Waste receptacles or by shredding. Reports not containing any SUNSI information can be disposed of through normal trash disposal.

8. Capability to *monitor individuals*

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

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

Access is limited by user's role(rights) with headquarters system administrator oversite.
Audit trails
Use of Passwords and User ID's.

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)? Provide number and name.

NRC-23, Office of Investigations Indices, Files and Associated Records.

b. If the Privacy Act System of Records is being modified, will the SOR notice require amendment or revision? Yes ___ 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)?

All of the above could have access to the data in the individual systems. Access is granted on a need to know basis. Users are assigned a logon ID and password and are limited to one of two roles, read-only or update for each individual system. There is no umbrella entry level.

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

Yes. User Manual, Systems Architecture Document, System Requirements Specification.

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

Yes. Authorized user access will still be in place for each individual system (AMS, EATS, and OIMIS). See 10. A.

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

The applications track users by LAN ID and date who add or update data. Audit trails will be reviewed periodically to minimize the impact of misuse.

e. Do other systems share data or have access to data in this system?
_✔__ Yes __ No. If yes, explain.

The Docket/Facility name is retrieved from the Reactor Program System (RPS). OIMIS, EATS and AMS will share some data fields electronically that are currently being shared manually.

f. Will other agencies share data or have access to data in this system (Federal, State, local, other)? ___ Yes _✔__ No. If yes, explain.

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? _✔__ Yes ___ No. If yes, explain.

Privacy Act clauses are cited in the Small Web Application 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: **Case Management System (CMS)**

Submitting Office: **Office of Information Services (for OI and OE)**

A. PRIVACY ACT APPLICABILITY REVIEW

_X_ Privacy Act is not applicable to EATS and AMS.

_X_ Privacy Act is applicable. OIMIS is covered under System of Records, NRC-23. 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.

Comments:

This PIA was previously submitted and reviewed under the name of ICASES in May 2005. My comments have not changed.

CMS is not a new system, but an umbrella title given to 3 currently existing systems (Allegation Management System (AMS), Enforcement Action Tracking System (EATS), Office of Investigation Management Information System (OIMIS)) that will now be web-based applications allowing data common to all 3 systems to be shared electronically. This common data is currently being shared manually on a need to know basis between the offices to perform their duties. The 3 systems, which will still remain separate, are being updated with the additional common data fields. No personal information will be shared. This will be accomplished by creating two additional tabs in each system. For example, the AMS will have tabs incorporated for EATS and OIMIS, and so on. When the tab is clicked a window will open displaying the shared data fields for that system. Data fields will only be populated if an allegation is substantiated and passed to OI for an investigation or moves forward for an enforcement action. The system security plan will address each subsystem individually. Separate access authorizations will still exist.

I spoke with system contacts from both OI and OE. OI confirmed that no information about an individual will be shared, only information from data fields that are already provided to OE. OIMIS is currently covered under Privacy Act system of records NRC-23, "OI Indices, Files and Associated Records." Information about an individual is not retrieved from OIMIS using an established name or personal identifier search. However, when information about an individual is needed, the text search is used to retrieve this information. No change to the current system notices will be required. AMS and EATS are not Privacy Act systems of records. Information is not retrieved by an individual's name or personal identifier from either system.

Reviewer's Name	Title	Date
Sandra S. Northern	Privacy Program Officer	May 10, 2006

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

___ No OMB clearance is needed.

___ OMB clearance is needed.

_X_ Currently has OMB Clearance.

Comments:

The Case Management System contains the Allegations Management System (AMS), Enforcement Action Tracking System (EATS), and the Office of Investigations Management Information System (OIMIS). The purpose of combining these three systems under one "umbrella" system is to replatform them from a legacy client/server application environment into a Web application environment on the NRC Internal Web site. The design of these applications will allow data common to all 3 systems to be shared electronically.

Allegation initial and follow up information may be collected from the public, and is reported to the NRC under 10 CFR Part 19.16a. This collection of information is covered under OMB clearance number 3150-0044.

Reviewer's Name	Title	Date
Christopher J. Colburn	Team Leader	May 24, 2006

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

___ Additional information is needed to complete assessment.

_X_ 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:

The National Archives and Records Administration required that all systems be scheduled whether they contain records or not. The information provided indicates that this system is a record keeping system, but does not contain records. Further information is required to understand why this record keeping system, does not contain records and to complete the

records evaluation so that an appropriate disposition schedule can be established for the system. However, the need for further records evaluation does not preclude moving forward with the system certification.

Reviewer's Name	Title	Date
Jeff Bartlett	Senior Records Management Analyst	5/16/06

D. BRANCH CHIEF REVIEW AND CONCURRENCE

_X_ 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: 05/25/2006
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.)

_____ Date: _____
John J. Linehan, Director, Information and Records Services Division

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

To: **Office of Information Services (for Office of Investigations and Office of Enforcement)**	Office Sponsor: **Guy Caputo, Director OI** **Michael Johnson, Director, OE**	
Reginald W. Mitchell, Director Business Process Improvement and Applications Division, OIS	Name of System: **Case Management System (CMS)**	
Kathy L. Lyons-Burke, CISSP Senior IT Security Officer (SITSO)/Chief Information Security Officer (CISO), OIS	Date Received: **04/27/2006**	Date Completed: **05/24/2006**
Noted Application Development and System Security Issues: The OIMIS subsystem is covered under Privacy Act system of records NRC-23. No information collection issues. Further information is required to complete the records evaluation so that an appropriate disposition schedule can be established for the system. However, the need for further records evaluation does not preclude moving forward with the system certification.		
Brenda J. Shelton, Chief Records and FOIA/Privacy Services Branch Office of Information Services	Signature: ***/RA/***	Date: 05/25/2006