ADAMS ML060300153

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: **12/12/2005**

A. GENERAL SYSTEM/APPLICATION INFORMATION

(See definitions at end of document)

1. Person completing this form:

Name	Title	Phone No.	Office
David Curtis	IT Specialist	415-6012	OIS

2. System owner:

Name	Title	Phone No.	Office
Myron Kemerer	Branch Chief	415-8735	OIS

3. What is the name of this system?

Enterprise Architecture Repository System

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

This system supports the Enterprise Architecture Program as well as the Information Security Program in the Agency and consists of the following 3 subsystems:

- HEART - website for the agency to look at how systems relate to each other and federal enterprise architecture.
- EAST - Accessible only to OIS Information Security Staff - maintains security information program data.
- IMINE - consolidated list of agency systems which includes System ID, System Acronym, System Name, Description, System In Use, Privacy Act System (Yes/No), MD 12.5 System Type, FIPS 199 Risk Level, NRC Office Name, and Contacts (Business Owner, Project Manager, ISSO)

EARS-AIS supports the NRC strategic goal to ensure excellence in agency management to carry out the NRC's strategic objective. Specifically, this system supports the strategy

of expanded electronic government.

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

__X_New System _____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 _X*__ No ___

*This system maintains only the name of employees identified as the system contacts (business owner, project manager, and ISSO).

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_X_

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 _X____

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 ____ 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 __X__

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.

This system will maintain data about the automated information systems in use throughout the agency. The information primarily deals with enterprise architecture data and security data. The system will also maintain the name of the employees identified as the system contacts (business owner, project manager, and ISSO).

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?

Yes. The system contacts provide the data that are maintained in the system.

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. Originally the data from the System Architect (an EA productivity database) and from ITSSTS, the security tracking database, will be incorporated into this system. Data will then be entered by the system business offices.

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?

Not Applicable.

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. The data related to persons names are in a document called EARS-AIS System Fields.xls and is contained in the EARS Rational ClearCase VOB

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

Yes it is both relevant and necessary for the purpose that the system was designed.

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?

Not Applicable.

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

Not Applicable.

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

Not Applicable.

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

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

b. Is a password or data description required? __X__ Yes _____ No.

If yes, explain.

To access sensitive data in the system a password is required. Some basic system information, including contact names will be accessible without a password.

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

a. What reports are produced from the system?

A report will be generated for any changes that have been requested to automated information systems since the last time that the database has been updated. Also reports of system names will be available.

b. What are the reports used for?

This report will be used by the change control board to evaluate change requests for approval, denial, or more information requested. System name reports will be provided to OMB for compliance reporting.

c. Who has access to these reports?

The system administrator of EARS as well as EA Team members and Security Team members will have access to the change request report. The systems names report will have a wider distribution to include OMB and the Office of the Inspector General (but will not contain personal information).

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 - database
Medium - electronic

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

Not Scheduled.

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

7 years - General Record Schedule 27: Enterprise Architecture Records
1 year - General Record Schedule 24: Files Related to Maintaining the Security of Systems and Data.

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)?

MD 3.53 NRC Records Management Program Handbook: Disposition of Electronic Records.

e. How long will produced reports be maintained?

Reports that are produced for systems change control will be generated on the day that the approval takes place and destroyed within 1 day of the approval or denial of change. Reports of system names will be produced for OMB and submitted to them for review (retention period unknown).

f. Where are the reports stored?

The systems change control reports will be maintained by the system administrator and kept in their possession for approval or denial and then destroyed once the inventory has been updated.

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

MD 3.53 NRC Records Management Program Handbook for the data. The reports that are produced by this system do not contain privacy information.

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

For EARS and IMINE subsystems, the reports that are generated do not contain sensitive information and are disposed of through regular trash disposal. For the EAST subsystem, the reports are disposed of in Classified and Sensitive Unclassified Waste receptacles.

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?

Not Applicable.

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.

Not Applicable.

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)?

System Inventory Data
System Administrator
Developer (contractor)
NRC Staff
System Owner
Security Data
NRC IT Security Team
IT Security Contractor
SITSO

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

No.

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

The data is broken into two major types: IT system security data and IT system inventory data. Most users will have access to all data related to the system inventory data. This portion contains basic information on systems and is not being restricted within the agency. All security related data will be restricted to the IT Security Team and the System Owners.

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

It is expected that the system will identify anyone attempting to modify data and this information will be tracked. Access to security data will require password authentication and also will be audited.

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

System Architect (Enterprise Architecture Productivity Tool) will retrieve inventory data from this system to perform modeling of systems.

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

Yes, this data must regularly be reported to OMB.

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 __X__ If yes, explain.

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: **Enterprise Architecture Repository System**

Submitting Office: **Office of Information Services**

A. PRIVACY ACT APPLICABILITY REVIEW

_X_ Privacy Act is not applicable.

____ Privacy Act is applicable. Currently covered under System of Records, NRC _____. 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:

EARS is a system developed to maintain information about NRC IT systems, not about individuals. The only information about an individual in the system is the name of the system contact(s). No other information about individual is maintained in the system. No information is retrieved by an individual's name or personal identifier.

I contacted David Curtis for clarification on a few answers. David agreed to add clarification by changing the following question answers to read:

Question A.4: This system supports the Enterprise Architecture Program as well as the Information Security Program in the Agency and consists of the following 3 subsystems:
HEART - website for the agency to look at how systems relate to each other and federal enterprise architecture.
EAST - Accessible only to OIS Information Security Staff - maintains security information program data.
IMINE - consolidated list of agency systems which includes System ID, System Acronym, System Name, Description, System In Use, Privacy Act System (Yes/No), MD 12.5 System Type, FIPS 199 Risk Level, NRC Office Name, and Contacts (Business Owner, Project Manager, ISSO).

EARS-AIS supports the NRC strategic goal to ensure excellence in agency management to carry out the NRC's strategic objective. Specifically, this system supports the strategy of expanded electronic government.

Question B.1: Yes*. *This system maintains only the name of employees identified as the system contacts (business owner, project manager, and ISSO).

Question E.1: Add another sentence to read: The system will also collect the name of the employees identified as the system contacts (business owner, project manager, and ISSO).

Question E.2.a: The system contacts provide the data that are maintained in the system.

Question E.2.b: Originally the data from the System Architect (an EA productivity database) and from ITSSTS, the security tracking database, will be incorporated into this system. Data will then be entered by the system business offices.

Question E.7.h: For EARS and IMINE subsystems, the reports that are generated do not contain sensitive information and are disposed of through regular trash disposal. For the EAST subsystem, the reports are disposed of in Classified and Sensitive Unclassified Waste receptacles.

Reviewer's Name	Title	Date
Sandra S. Northern	Privacy Program Officer	January 30, 2006

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

_X_ No OMB clearance is needed.

____ OMB clearance is needed.

____ Currently has OMB Clearance.

Comments:

This PIA does not contain information collections, based on the information provided that no information is being collected from persons who are not Federal employees or from Federal contractors. Therefore, no OMB clearance is needed.

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

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

_X_ 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:

The National Archives and Records Administration requires that all systems be scheduled. Therefore, an appropriate disposition schedule will have to be established for this system. The general record schedules identified in this document may be able to be applied to portions of this system. Others may be covered by different sections of the GRS or may need agency specific schedules developed. Further information is required to identify specific pieces of the system and to make a determination regarding what schedules apply to each. 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	02/07/2006

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: _____**R/A**_____ Date: 02/07/2006
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: (Sponsoring Office) **Office of Information Services**	Office Sponsor: **Myron Kemerer**	
Reginald Mitchell, Director Director Business Process Improvement and Applications Division, OIS	Name of System: **Enterprise Architecture Repository System**	
Kathy L. Lyons-Burke, CISSP Senior IT Security Officer (SITSO)/ Chief Information Security Officer (CISO), OIS	Date Received: 01/20/2006	Date Completed: February 7, 2006

Noted Application Development and System Security Issues:

The Privacy Act is not applicable.

No OMB clearance is needed.

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, OIS	Signature: **R/A**	Date: **02/07/2006**