

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: 03/17/2006

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

2. System owner:

Name	Title	Phone No.	Office
Belkys Sosa	Business Project Manager	301 415-1724	EDO

3. What is the name of this system?

Foreign Travel System

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

The purpose of this effort is to develop a Web base application that will allow the major NRC offices to enter, coordinate, monitor, and approve foreign travel. The Commission directed the EDO to develop a process for monitoring and approving foreign travel throughout the agency to ensure that NRC representation at international meeting is coordinated and conducted as efficiently and effectively as possible.

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

New System 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

If yes, give category of individuals (e.g., Federal employees, Federal contractors, general public, etc.)

Federal employees, Federal contractors

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 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? **N/A**

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 _____

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 only contain travel data as it relates to foreign travel, meetings held and where, estimated cost, purpose of the trip as it relates to what organization, committee, and a trip report of the meeting, and the name of the traveler.

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, information in E.1.a. is provided by the lead traveler.

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

No

- 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?

N/A

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 documentation is stored in the Rational ClearCase VOB.

System Architecture Document

- 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?

No

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

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

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.

Although the capability exists to retrieve trip information by lead traveler's name, information would routinely be retrieved by NRC office or trip date.

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

Access authorization is granted by the system administrator

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

- a. What reports are produced from the system?

Trip summary and statistical reports.

- b. What are the reports used for?

Provide the office with travel plans and the outcome of the trip with a summary report of the meetings.

- c. Who has access to these reports?

The office that sponsors the trip and the EDO.

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?

Records Schedule Number	Description of Records	NARA Authorized Retention Period
N/A	Database records, inputs, outputs, and system programming	Unscheduled
GRS 20-1c.	Files/Records Relating to the Creation, Use, and Maintenance of Computer Systems, Applications, or Electronic Records c. Electronic files or hard-copy printouts created to monitor system usage, including, but not limited to, log-in files, password files, audit trail files, system usage files, and cost-back files used to assess charges for system use.	Delete/destroy when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes.
GRS 20-11a.	Documentation Data systems specifications, file specifications, codebooks, record layouts, user guides, output specifications, and final reports (regardless of medium) relating to a master file or data base that has been scheduled for destruction by the GRS or a NARA-approved disposition schedule.	Destroy or delete when superseded or obsolete, or upon authorized deletion of the related master file or data base, or upon the destruction of the output of the system if the output is needed to protect legal rights, whichever is latest.
GRS 24-4a.	System Backups and Tape Library Records	(1) Delete/destroy incremental backup tapes when superseded by a full backup, or when no longer needed for system restoration, whichever is later.

GRS 24-5a.	System Security Plans and Disaster Recovery Plans	Destroy/delete 1 year after system is superseded.
------------	---	---

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

At this time the data will be retained until no longer needed.

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

See 7.b above

e. How long will produced reports be maintained?

Mostly, one or two years.

f. Where are the reports stored?

File cabinets (lockable and un-lockable)

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?

They will be disposed of in accordance with the GRS/NARA schedule.

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 oversight.
Audit Trails
Use of Password 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.

N/A

- 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 system. 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.

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

Yes, User Manual, System Architecture Document, System Requirements Specification, Foreign Travel System.

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

Yes. Access is restricted to Roles/rights as assigned by the system administrator. Users are granted full access to their data and read-only to other data in the system.

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

The application tracks users by LAN ID. 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.

- 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.

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: **Foreign Travel System**

Submitting Office: **Office of the Executive Director of Operations**

A. PRIVACY ACT APPLICABILITY REVIEW

- 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:

Art Davis and Douglas Weaver confirmed this will be a tracking system for information on NRC foreign travel. The information will be used to show that NRC is properly represented at international meetings/conferences and to assist in the coordination and follow-up of planned and future trips. The only data maintained in the system "about" an individual will be a traveler's name. Travelers can be NRC employees and/or contractors. If more than one traveler is attending from NRC, only the name of the designated lead traveler will be captured. The names of other NRC attendees will be included in the trip comments/summary. The lead traveler will provide the information to be captured in the database regarding a particular trip. No information about the "general public" will be collected or maintained in the system.

Although the capability exists to retrieve information by a traveler's name the system is not keyed to the individuals listed in the "lead traveler" (contact person) field of this database because the agency's purpose for including the name of the lead traveler is essentially administrative and not to be used to obtain information "about" that individual.

Reviewer's Name	Title	Date
Sandra S. Northern	Privacy Program Officer	March 29, 2006

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

No OMB clearance is needed.

OMB clearance is needed.

Currently has OMB Clearance.

Comments:

Some non-government information (e.g., contractor name) regarding Federal contractors is gathered to populate the Foreign Travel System. However, the primary source of data for this system is obtained from the agency planning foreign travel through their submission of pre-trip coordination reports and post-trip meeting reports. In addition, no more than 9 contractors are ever expected to participate in foreign travel annually. Because the data generated to populate the Foreign Travel System database is obtained by the agency offices from existing agency sources, no OMB clearance is required.

Reviewer's Name	Title	Date
Christopher J. Colburn	Team Leader	March 30, 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:

Extensive material provided on computer artifacts that are covered by NARA General Record Schedules. However, information on retention of program specific information not provided. Further dialog and information will be required to establish appropriate schedule for material being captured in the system. However, the need for further records management evaluation does not preclude moving forward with certification of this system.

Reviewer's Name	Title	Date
Jeff Bartlett	Senior Records Analyst	3/29/2006

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: 03/30/2006
Brenda J. Shelton, Chief
Records and FOIA/Privacy Services Branch

E. DIVISION DIRECTOR APPROVAL OF PRIVACY IMPACT ASSESSMENT

(Approval required if this "does constitute a Privacy Impact Assessment required by the E-Government Act of 2002")

_____ 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 the Executive Director for Operations	Office Sponsor: Belkys Sosa	
Reginald W. Mitchell, Director Business Process Improvement and Applications Division, OIS	Name of System: Foreign Travel System	
Kathy L. Lyons-Burke, CISSP Senior IT Security Officer (SITSO)/Chief Information Security Officer (CISO) Office of Information Services	Date Received: 03/20/2006	Date Completed: 03/30/2006
<p>Noted Application Development and System Security Issues:</p> <p>No Privacy Act issues.</p> <p>No information collection issues.</p> <p>Further dialog and information will be required to establish appropriate schedule for material being captured in the system. However, the need for further records management evaluation does not preclude moving forward with certification of this system.</p>		
Brenda J. Shelton, Chief Records and FOIA/Privacy Services Branch, OIS	Signature: <i>/RA/</i>	Date: 03/30/2006