2008 Privacy Impact Assessment

Name of Project: Archival Declassification Redaction and Tracking System and Unclassified Declassification and Redaction System

Project's Unique ID:
ADRRES and URTS

Legal Authority(ies):
44 U.S.C. Chaps 21, 29, and 31

Purpose of this System/Application:
ADRRES allows for the indexing of all classified archival document at NARA. This includes documents under going systemic declassification, as well as documents requested under the freedom of information act (FOIA). The system also allows scanning and subsequent redaction of classified documents requested under the FOIA, and tracks these requests throughout the FOIA process. URTS has the same function but is used for unclassified documents.

Section 1: Information to be Collected

1. Describe the information (data elements and fields) available in the system in the following categories:

a. **Employees**
   User ID and password
b. **External Users**
   N/A
c. **Audit trail information (including employee log-in information)**
   The subsystem audits all user logins, all administrative functions and all application user events such as viewing, inserting, and updating information.
d. **Other (describe)**
   Contact information of FOIA requesters is input and maintained in the system.

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources?

a. **NARA operational records**
   FOIA requests and responses are both scanned into ADRRES and URTS.
b. **External users**
   N/A
c. **Employees**
   N/A
d. **Other Federal agencies (list agency)**
   Both systems contain scanned archival documents, which are received from Federal agencies consistent with approved records schedules. Some records submitted

contain personally identifiable information.

e. **State and local agencies (list agency)**
   N/A
f. **Other third party source**
   N/A

Section 2: Why the Information is Being Collected

1. **Is each data element required for the business purpose of the system? Explain.**
   Yes. In order to properly track and response to FOIA requests the contact information is necessary.

2. **Is there another source for the data? Explain how that source is or is not used?**
   No.

Section 3: Intended Use of this Information

1. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

No.

2. Will the new data be placed in the individual's record?

N/A

3. Can the system make determinations about employees/the public that would not be possible without the new data?

Other than the fact that a FOIA request has been made, no new determinations can be made.

4. How will the new data be verified for relevance and accuracy?

N/A

5. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

Access to the system is controlled by username and passwords. It should also be noted that this system is a classified system and users are required at a minimum have a top secret clearance in order to access the system.

6. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

See question five above.

7. Generally, how will the data be retrieved by the user?

In the case of a declassification project file, data is typically retrieved by the project number. FOIA requested are retrieved by the requesters name or case file number.

8. Is the data retrievable by a personal identifier such as a name, SSN or other unique identifier? If yes, explain and list the identifiers that will be used to retrieve information on an individual.

Data can be retrieved by name.

9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

The log of FOIA requests can be searched by name to identify any requests made by an individual.

10. Can the use of the system allow NARA to treat the public, employees or other persons differently? If yes, explain.

No.

11. Will this system be used to identify, locate, and monitor individuals? If yes, describe the business purpose for the capability and the controls established explain.

No.

12. What kinds of information are collected as a function of the monitoring of individuals?

N/A

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

Access to data in the system is limited by user access control lists or ACL's. Any unauthorized monitoring or activities would be captured in the system log files which are monitored daily.

14. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?

No.

Section 4: Sharing of Collected Information

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

NARA employees and contractors working with declassification review and FOIA.

2. How is access to the data by a user determined and by whom? Are criteria, procedures, controls, and responsibilities regarding access documented? If so, where are they documented (e.g., concept of operations document, etc.).

The system administrator creates user accounts for each user. All users must posses a top secret security clearance to use the system.

3. Will users have access to all data on the system or will the user's access be restricted? Explain.

The system administrator along with the ISSO and system managers defines access to various datasets.

4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those who have been granted access (please list processes and training materials)?

System managers and owners have the ability to audit user logs, system level events and all user activities.

5. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

Contractors are involved in the design, development and maintenance of the system. NARA managers control access and monitor all system changes through a well defined Configuration Management Control Process or CM. Contractors have the appropriate PIA clauses in their contract.

6. Do other NARA systems provide, receive or share data in the system? If yes, list the system and describe which data is shared. If no, continue to question 8.

No.

7. Have the NARA systems described in item 6 received an approved Security

Certification and Privacy Impact Assessment?

N/A

8. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

N/A

9. Will other agencies share data or have access to the data in this system (Federal, State, Local, or Other)? If so list the agency and the official responsible for proper use of the data, and explain how the data will be used.

If a document is referred to an equity holding agency, data may be shared with that agency in order to facilitate the referral. Other agencies do not have direct access to the systems.

Section 5: Opportunities for Individuals to Decline Providing Information

1. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how can individuals grant consent?

In the case of FOIA requests, NARA is required to respond via mail. As such, a mailing address is necessary.

2. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?

N/A

Section 6: Security of Collected Information

1. How will data be verified for accuracy, timeliness, and completeness? What steps or procedures are taken to ensure the data is current? Name the document that outlines these procedures (e.g., data models, etc.).

For FOIA requests, the data is provided by the requestor. Accuracy and timeliness and completeness of the data in provided by the FOIA requestor.

2. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

N/A

3. What are the retention periods of data in this system?

Records in ADRRES and URTS are unscheduled and are not deleted.

4. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented? Cite the disposition instructions for records that have an approved records disposition in accordance with, FILES 203. If the records are unscheduled, they cannot be destroyed or purged until the schedule is approved.

N/A

5. Is the system using technologies in ways that the Agency has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)? If yes, describe.

No.

6. How does the use of this technology affect public/employee privacy?

There is no technological affect on public/employee privacy.

7. Does the system meet both NARA's IT security requirements as well as the procedures required by federal law and policy?

Yes, the systems are Certified and Accredited (C&A) by the mandated authorities and comply with all Federal laws and policy.

8. Has a risk assessment been performed for this system? If so, and risks were identified, what controls or procedures were enacted to safeguard the information?

Yes, risks have been assessed and a PO&A was completed during the last certification.

9. Describe any monitoring, testing, or evaluating done on this system to ensure continued security of information.

This system is in full compliance with Federal guideline for classified systems and NARA's security testing and certification process/procedures.

10. Identify a point of contact for any additional questions from users regarding the security of the system.

Leo Scanlon, NARA ISSO, 7-0752

Section 7: Is this a system of records covered by the Privacy Act?

1. Under which Privacy Act systems of records notice does the system operate? Provide number and name.

This system operates under NARA Privacy Act system notice, NARA 7, Freedom of Information Act (FOIA) Request Files and Mandatory Review of Classified Documents request Files.

2. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

N/A

Conclusions and Analysis

1. Did any pertinent issues arise during the drafting of this Assessment?

No.

2. If so, what changes were made to the system/application to compensate?

N/A

See Attached Approval Page

Once the Privacy Impact Assessment (PIA) is completed and the signature approval page is signed, please provide copies of the PIA to the following:

IT Security Manager
Privacy Act Officer

The Following Officials Have Approved this PIA

1) **ADRRES System Owner**

Jeanne Schauble (Signature) 8/28/08 (Date)
Jeanne Schauble, NWMD

URTS System Owner

[signature] (Signature) 8/28/08 (Date)
David Mengel, NWCTF

2) **Senior Agency Official for Privacy (or designee)**

[signature] (Signature) 9/4/08 (Date)
~~**Ramona Oliver**~~, **NGC**
GM/ Gary M. Stern

3) **Chief Information Officer (or designee)**

Martha Morphy (Signature) 9/5/08 (Date)
Martha Morphy, NH