Privacy Impact Assessment

Name of Project: Researcher Registration System

Project's Unique ID: RRS

Legal Authority(ies): 44 U.S.C. 2108, 2111 note, and 2203(f)(1) and 36 CFR Chapter XII, 1254.6-8

Purpose of this System/Application: a. The Researcher Registration System (RRS) provides registration of users and access to secure research rooms that house original collection and non-classified information by issuing a researcher a research card. This registration and badge access control system is located at both the National Archives Building in Washington, DC (Archives I) and the National Archives at College Park (Archives II) and runs on a separate segment from the NARANET. The system is a registration and badge access control system that enables NARA to track researcher personal information and researcher access to research materials, including visits to either facility. The system accomplishes this task through the use of magnetic cards, card terminals, and databases.

Section 1: Information to be Collected

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

a. Employees – Unique login and password

b. External Users - Identifying information provided by the individual researcher seeking a research card. NARA does not supplement this information. Includes the data elements outlined in 2b below.

c. Audit trail information (including employee log-in information) - Audit tools create, maintain, and protect a trail of actions of users and administrators that trace security relevant events. Operating system logs are maintained and reviewed periodically.

d. Other (describe) N/A

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

a. NARA operational records -Researcher identification cards contain name, address, and original research interests of the researcher.

b. External users -The following information is provided by the researcher apply for a research card:

Title
First name
Middle initial
Last name
US address
Foreign address or US temporary address
US phone number
Photo
Identification type (government issued id)
Identification issuer and number (in relation to government issued id)
Badge number
Badge active
Expiration date
Print date
Photo date
Last edit date
Research topic
Specific records
Building
Opt-out of mailings
Have used website
Staff note
Transactions for research rooms equipped with badge readers

c. **Employees- N/A**
d. **Other Federal agencies (list agency) – N/A**
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. Each element relates to researcher identification, the reason for the visit, and tracking transactions in the research room.

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. Currently, no aggregate data is produced. If produced in the future, aggregate data will not identify an individual.

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?

N/A

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?

N/A

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

N/A

7. Generally, how will the data be retrieved by the user?
Researchers enter their own information. Authorized users can search in any text filed, ıncluding name and NARA Researcher Identification 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 any field, including name and identification number. However, that data is usually only retrieved by personal identifier when there is a business need to do so. Other extracts are for statistical purposes.

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

Reports on individuals normally include the following information: first name, middle initial, last name, US address, foreign address or US temporary address, phone number, photo identification type, identification issuer and number, badge number, badge active, expiration date, print date, photo date, last edit date, research topic, specific records, building, and research room transactions.

These reports are usually only generated to assist NARA in maintaining intellectual control over archival holdings and/or to refer related information to the Office of Inspector General, or other law enforcement agencies if original records are determined to be missing or mutilated. For those requesters who choose to receive mailings from NARA, we use these reports to disseminate information related to events and programs of interest to NARA's researchers. We also use the reports to measure customer satisfaction with NARA services. Aggregate data may be compiled from these reports for the purposes of review, analysis, planning and policy formulation related to customer service staffing and facility needs. NARA's reference staff can receive restricted information such as spelling of the last name, address, and phone number in order to facilitate reference services. The ability to generate these reports is limited to authorized staff using a user id and password.

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.

The system can identify the last research room where a person had a transaction. This function is only accessible to the system administrator and selected supervisory personnel.

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

Such reports include the identification of the research room visited, the time of visit and the date. All such transactions are limited to authorized users who have been granted access to this function.

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

Only authorized users of the system have access to this information.

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)?

Contractors, users, managers, system administrators, developers, and security personnel will have access to the data in the system. Access is based on standards and procedures associated with user ID (identification), password (authentication), and access privileges (e.g., role-based access to systems, databases, data fields, and privileges to view, create, change and delete data).

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.).

Access is determined by the system administrator based on job duties. Technical controls protect against unauthorized access to, or misuse of, e-RRS QIP resources and facilitate detection of security violations.

Authentication to RRS involves users going to workstations and completing a form online to receive a registration card. These workstations need no authentication to be used. Once a registration request is completed on the workstation the registration desk is notified of the new record where users supply government issued identification to receive their card.

Logical access control is based on standards and procedures associated with user ID (identification), password (authentication), and access privileges (e.g., role-based access to systems, databases, data fields, and privileges to view, create, change, and delete data).

Logical Access to the RRS system uses NARANET. Please refer to the NARANET PIA for more information on logical access controls.

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

Public users only have access to the information they submit. Internal user access is limited to the information necessary to perform their job. Only the system administrator and authorized NARA users have unrestricted access to all the information in RRS.

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)?

Technical controls protect against unauthorized access to, or misuse of, RRS resources and facilitate detection of security violations by generating audit logs to record users' activities and warn of anomalous conditions in the network. Audit tools create, maintain, and protect a trail of actions of users and administrators that trace security-relevant events to an individual, ensuring accountability.

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?

N/A

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.

Research badge numbers with no other information are sent to the Copy Card System. Badge numbers in isolation cannot identify individuals. This export of data increases researcher convenience by allowing them to use the research badge as a copy card.

The records retrieval (pull) database in use in the textual research room in College Park uses the badge number to find the researcher's name and photo. The name and badge number are stored in the pull database. These pieces of information have always been part of the pull slip system. The photo is only displayed on the screen momentarily in order to help staff be sure that the pull is being submitted for the correct researcher. The pull database resides in the same instance of SQL server as the badging software.

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.

N/A

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?

A privacy notice outlining the use of the information and the OMB authorization for the collection is shown before the registration form is filled out. Providing the information is voluntary, but researchers who do not provide the information will not be able to do research at the National Archives.

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

Yes. NARA may use the information in RRS to contact a researcher concerning the revocation of their research room privileges. This information is maintained in a properly published Privacy Act system of records, which authorizes individuals to gain access to their own records. Moreover, if NARA revokes a researcher's research room privileges, he or she has the right to appeal such determinations in accordance with 36 CFR 1254.48-52.

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.).

Researchers provide information about themselves. We assume it is accurate, timely and correct at the time of collection. Information provided by the researcher is verified against the government issued identification submitted to support the application. Information is updated, if needed, when the research badge is renewed or if the researcher informs NARA of a change in their personal information. Research badges are valid for one year from date of issue. The researcher must initiate the renewal and provide the appropriate supporting documents.

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?

The RRS system operates over a private, segmented LAN at both of the Archives' facilities. This segmented LAN does not provide for any interconnectivity of devices that are not defined within the access control list. The system is stand-alone and does not need to interconnect with other systems in order to function.

The hardware components of the system are composed of servers, workstations, and Identicard readers. Each of these hardware components have been defined within the Access Control List, and access between hardware devices is facilitated by a router. The software interface is a COTS product that controls badging and access.

The hardware resources that access the RRS are clearly spelled out in the access control lists at both archives facilities. Only resources that are located at either Archives I or Archives II can be added to the RRS, as the system does not provide any WAN connectivity. The resources that are connected to this RRS do not require connectivity to any other Major Application or General Support System. For this reason, the segmented LAN containing the RRS remains virtually distinct from the NARA LAN and any WAN connections.

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

Researcher application files are temporary records and are destroyed in accordance with the disposition instructions in the NARA records schedule contained in FILES 203, the NARA Files Maintenance and Records Disposition Manual.

1418-1	Researcher Application Forms.	
	c. Researcher Registration System Database.	
	(1) Annual snapshot of entire database maintained offline.	Destroy when 25 years old. (N1-64-02-3, item 1)
	(2) Live data maintained on servers.	Delete when 3 years old. (N1-64-02-3, item 2)

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 that cannot be destroyed or purged until the schedule is approved.

See NARA Records Disposition Manual (FILES 203) 1418-1c above.

Reports are deleted after they have been provided to authorized users.

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?

No.

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

Yes, to a large degree it meets those requirements that are applicable specifically to RRS. NARANET is the GSS that provides many of the security controls for the systems that reside on it, including RRS. NARA's IT security requirements are based on Federal law, policy, and procedures.

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?

The last formal risk assessment of RRS was completed in March, 2007. Identified risks requiring mitigation are tracked through a POAM to ensure resources are allocated to resolve identified weaknesses.

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

NARA conducts vulnerability scans on all network devices on a monthly basis according to a predefined schedule. A quarterly report of open vulnerabilities is compiled and analyzed. In addition, a subset of NIST 800-53 controls are tested for NARA systems on an annual basis.

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

Leo Scanlon, NHI, AII, 301-837-0752

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 of records notice NARA-1, Researcher Registration Records

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

The Privacy Act system notice covering this system has been revised consistent with the new functionality of this system.

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

The Following Officials Have Approved this PIA

(Signature) 9/9/08 (Date)

Robert Coren, NWCC
RRS System Owner/Manager
8601 Adelphi Rd, Room 3400
College Park, MD 20740-6001
301-837-1992

(Signature) 9/10/08 (Date)

Gary M. Stern, NGC
Senior Agency Official for Privacy
8601 Adelphi Rd, Room 3110
College Park, MD
301-837-2024

(Signature) 9/11/08 (Date)

Martha Morphy, NH
Chief Information Officer
8601 Adelphi Rd, Room 4400
College Park, MD
301-837-1992