Privacy Impact Assessment (PIA)

Name of Project: Researcher Registration System (RRS)

Project's Unique ID: RRS

Legal Authority(ies):	44 USC 2108, 2111 note, and 2203(f)(1) and 36 CFRChapter XII, 1254.6-8

Purpose of this System/Application: The Researcher Registration System (RRS) provides registration of users and access to secure research rooms where original permanently-valuable non-classified records of the Federal Government are made available to the public. The system collects personal information and issues an identification card to the researcher. 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, Maryland (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 which research rooms authorized researchers are going throughout the research center, and records this data for both facilities. The card issuance portion of the registration process captures certain personally-identifiable information, and stores that data for periods of time as specified in the NARA Records Retention schedule. The cards themselves use a magnetic strip on the back of the card, and the cards are swiped when a researcher enters and exits the research center, and is also swiped once daily when the researcher enters any one of the research rooms to record their visit. The system serves both a security purpose as well as several administrative purposes.

Section 1: Information to be Collected

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

Employees		N/A
External Users		name, address, phone number, proof of ID, photograph
Audit trail information (including employee log-in information)		Yes, access limited to staff in the Researcher registration office
Other (describe)		

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

NARA operational records		for card renewals only
External users		All information provided by external users
Employees		n/a
Other Federal agencies (list agency)		n/a
State and local agencies (list agency)		n/a
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. This is the basic information to establish the identity of applicants for researcher identification cards.

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?

Yes, but the data is for the sole purpose of identifying applicants for researcher ID cards.

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

Yes, in the system determines who among the public is authorized to enter the research center.

4. How will the new data be verified for relevance and accuracy?
The data is provided by the individual and with photographic proof of ID, the information is deemed accurate in the absence of conflicting information.

5. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?
Not consolidated

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

7. Generally, how will the data be retrieved by the user?
Data is searchable by most fields, the most common being the ID number or name.

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 retrieved by personal identifier when there is a business need to do so. Other extracts are for statistical purposes and do not identify individuals.

9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?
We do not produce reports on individuals unless required to by the OIG or law inforcement agencies, which is extremely rare.

10. Can the use of the system allow NARA to treat the public, employees or other persons

differently? If yes, explain.
The system determines whether a person is authorized to use records at Archives 1 and Archives 2.

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.
Using a card swipe at the guard's station, the system records which research rooms are visited by whom and when they visited the first time each day. The card swipe also records each instance of the individual entering and leaving the research center.

12. What kinds of information are collected as a function of the monitoring of individuals?
The system monitors each time the researcher enters or leaves the researcher center. and the first time they enter each research room each day.

13. What controls will be used to prevent unauthorized monitoring?
Monitoring is electronic. The only human interface is with the swiping of the cards. The policy of the division is to refuse all but lawful requests for information from the system. For example. we would refuse to provide information on an employee of a business if requested by the person's supervisor. The person could file a FOIA but to my knowledge that has never been tried.

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

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)?
The data is available to members of the employees in the Registration Office, the system administrator. RD-DC customer service managers, and to the one contractor technician who has serviced the equipment and software for the past 10 years. The information might also be available to NARA's computer support contractor but that is highly unlikely.

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.). Are safeguards in place to terminate access to the data by the user?

Access is determined by the customer service coordinator who informs the system administrator that a new person in the office requires access. Likewise, when someone leaves and exits with NA 3009 form, the customer service coordinator or system administrator signs off that the person's access to the RRS has been terminated. There is a concept of operations document for the RRS. There are also written procedures within the office governing these matters.

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

The users of the system have access to all of the information.

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)? How will these controls be monitored and verified?

There is an audit trail to document unauthorized browsing. The written procedures used during training emphasize that unauthorized browsing is forbidden.

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?

The system development took place in 1999. There is still the same contractor maintaining the system under an O&M contract. If inserting the Privacy Act clause was the common practice of NH at the time, then it was done: if not, it wasn't. I do not have access to the contract file.

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 7.

The pull and refile system share the card ID number. The debit card system also uses the card number but has no access to any of the data. As of November 2010, the ID card also has a linkage with

NARA's wireless internet system (wi-fi). The card number serves as a user ID and the staff issue each researcher a temporary password which the user changes upon logging onto the wi-fi system. Because it is a free pblic system, no privacy is possible for users of the system, and this is spelled out in the terms and conditions.

7. Have the NARA systems described in item 6 received an approved Security Certification and Privacy Impact Assessment?

8. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?
The interface doesn't share any of the personal information.

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.
No, except as needed for law enforcement purposes.

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?
Individuals can decline to provide the information, but they will not be issued a researcher ID card and are therefore prevented from conducting research at NARA.

2. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
The person can appeal the decision up to review by the Archivist of the United States.

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.).

The data is provided by the person being issued the researcher ID card and is presumed to be accurate. The cards are issued for a period of one year, and then must be renewed, at which point the personal information is validated again. 36 CFR 1254 describes the process for applying for a researcher ID card and the period it is effective.

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?

There is a second site at A1. The Customer Services Manager is in charge of both locations and oversees the operation of both sites. The same set of guidelines applies to both locations. The system resides at Archives II, in the computer room.

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

The applications are maintained for 25 years, then destroyed. Other parts of the RRS database are maintained 2 to 5 years, depending on the series.

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.

The records are destroyed in accordance with Files 203 sections 1418-1c(1) and 1418-6.

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?

Federal regulations require that prospective researchers visiting a NARA research room provide proper and legal documentation in order to be admitted to do research. Any information provided to obtain a researcher ID card is done completely voluntarily. We do not share the information except when legally required to do so by the OIG or a government law enforcement organization, and then only with the NARA Privacy Officer's and/or Office Head's approval.

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

We've responded to each of NH's security concerns.

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. The major risk is that the servers handling the system fail. When that happens, we revert to the paper based system of issuing ID cards until service is restored. Normally its failure is linked to a failure of the NARANET.

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

There is an audit trail to cover browsing the records. We carried out scenarios with the Information Security staff in 2008 or 09.

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

Eric Chaskes is the system administrator and most familiar with the operation of the system. His office is in Rm 1000.

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.

System 1: Records relating to Researcher Applications

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

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?

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	
System Manager (Project Manager)	
(Signature)	9-20-2012 (Date)
Name: Robert W. Coren	
Title: Senior Archivist. Customer Serevice (RD-DC)	
Contact information: 301-837-1620	
Senior Agency Official for Privacy (or designee)	
(Signature)	9/14/12 (Date)
Name: Gary M. Stern	
Title: General Counsel & SAOP	
Contact information: 301-837-3026	
Chief Information Officer (or designee)	
Michael Wash (Signature)	9.12.12 (Date)
Name:	
Title: CIO	
Contact information:	