Privacy Impact Assessment

Name of Project: Access Control (Badging and Access) System
Project's Unique ID: B&A

Legal Authority(ies): 44 U.S.C. 2104

Purpose of this System/Application:

The Badging and Access System provides the appropriate individuals access to NARA facilities. The Badging System provides a means in which user information is entered onto the laminated badge. The Access System is the physical system that reads the laminated Identification badge and allows/denies access depending on access rights. The Badging System is a stand-alone system connected to a digital camera and printer. The Access System is also a stand-alone system. Four workstations are connected with dedicated connections directly to the system.

Section 1: Information to be Collected

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

a. Employees

The Badging System collects the name of the person seeking a NARA badge. The system also assigns each user an identification number.

The Access System collects the following information concerning NARA employees, contractors and volunteers: name, date of birth, height, weight, hair and eye color, and assigned card number.

b. External Users – N/A

c. Audit trail information (including employee log-in information)

The Badging & Access System allows authorized personnel to track individuals using name and or card number. Audit tools create, maintain, and protect a trail of actions of users and administrators that trace security-relevant events to an individual, ensuring accountability. Currently, audit logs are not checked to trace actions of users.

d. Other (describe) - None

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

a. NARA operational records - N/A

b. External users – N/A

c. Employees

Employees provide their legal names and other identifying information.

d. Other Federal agencies (list agency) - N/A

e. State and local agencies (list agency) - N/A

f. Other third party source

The Badging & Access System is populated with pre-programmed identification numbers that are assigned as badges are issued to individuals. Other information in the system comes from personnel forms and state issued identification cards that support the information provided by the employee, contractor, or volunteer seeking a NARA badge.

Section 2: Why the Information is Being Collected

1. Is each data element required for the business purpose of the system? Explain.
Yes, each date element is necessary to positively identify the individual and to provide a badge giving the individual access to the building.

2. Is there another source for the data? Explain how that source is or is not used?

N/A

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?

No.

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

No.

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?

Authentication to the Access System is controlled at two layers. First the user must log onto the specific workstation that is hard-wired to the Access System. This access is via individual username/password pairs. Second the user must know a common password to gain access to information in the system. Authentication to the Badging System involves logging into the individual workstation from a stand-alone PC.

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.

Yes, information in the Badging & Access System can be retrieved by an individual's name and/or unique identification card number. The identification number is generated by the system.

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 system allows for the creation of tracking reports on individuals who have been assigned a NARA access badge. That report provides information concerning the movement of the badge holder within the building. It provides information concerning the areas the individual entered and the time of such entry. This information is usually used by security personnel or the Inspector General for investigative purposes.

Audit tools create, maintain, and protect a trail of actions of users and administrators that trace security-relevant events to an individual, ensuring accountability. Currently, audit logs are not checked to trace actions of users.

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

Yes. The Badging and Access System can be used to allow NARA to treat the public, employees, or others differently. By granting a badge, we allow employees varying degrees of access to locations within the building. That access is determined based on the individuals' job related duties and the approvals granted by management and the personnel security staff. By denying a badge, the system restricts public access to restricted or employee only areas.

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.

Yes, the system tracks individual badge holders when they enter a location via access control card.

The system contains the ability to trail the actions of users and administrators that trace security-relevant events to an individual, ensuring accountability.

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

Name, card number, location(s) entered, and time of such entry.

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

Access to the Badging and Access System is restricted to Security Personnel. Authentication to the Access System is controlled at two layers. First the user must log onto the specific workstation that is hard-wired to the Access System. This access is via individual username/password pairs. Second the user must know a common password to actually log onto the system. Moreover, authorized users of the Badging and Access System are subject to the NARA wide personnel security controls. NARA personnel security controls are described in section 1 of NARA IT Security Handbook. Please refer to NARA IT Security Handbook, Operations Controls for more information.

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 system administrator and authorized users have access to the Badging and Access System. Please reference question 7 (Attributes of Data section) and question 8 (Maintenance and Administrative Controls section) on safeguards.

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 determines the user's access to the system based on the user's job and their need for access to the system in order to perform that job. Responsibilities are outlined in the Concept of Operations document for the Badging and Access System as well as the System Security Plan.

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

Access to information in the system is restricted by the system administrator based on job duties and need to know.

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)?

Authorized users of the Badging and Access System are subject to the NARA wide personnel security controls. NARA personnel security controls are described in section 1 of NARA IT Security Handbook, Operations Controls. This protocol reminds users to only use the system for the purpose for which it was created and consistent with their authorized duties. This message is reinforced in annual security training and is reinforced with issuance of NARA policy guidance on this topic.

The system also contains the ability to trail the 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?

No. Contractors installed the system, however, input and maintenance is performed by NARA staff with personnel security duties.

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.

The Access Control System is connected to fire alarm. If the fire alarm is triggered in a certain area the doors leading out are unlocked. Besides the fire alarm system, the Access Control System does not connect to any other system. All connecting workstations/sensors are directly connected. The Fire Alarm panel and the access control system share no data; it is a simple dry contact from the fire panel directly to the doors in the emergency exit pass to ensure they are unlocked in the event of an emergency.

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

N/A – The fire alarm does not require a PIA. The connection between the fire alarm and the Access System is evaluated in the Badging and Access System Security Plan of July 31, 2003.

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

The System Administrator for the Badging and Access System is responsible for protecting the privacy rights of the public and employees affected by the interface. NARA's Senior Agency Official for Privacy is responsible for ensuring compliance with the privacy rights of the public and NARA employees.

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.

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?

Submission of the requested information is voluntary; however, refusal to provide such information will result in the inability to obtain an access control card. Refusal to provide this information may also result in the inability to perform certain job related tasks because an individual will be unable to gain access to certain areas of the building where entry requires an access card.

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.).

Information in the system is provided by the individual seeking a NARA access badge (employee, contractor or volunteer). The individual provides documentation (drivers license, employment form, SF-50, etc) that is needed to verify their identity. We assume the individual is providing accurate, timely and complete information regarding themselves. Secondary documents are assumed correct if they have not expired.

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?

Credentials and passes 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.

649	**Credentials Files**	
649-1	Identification credentials including cards, badges, photographs, and property, visitors' passes, and other identification credentials.	Destroy credentials 3 months after return to issuing office (GRS 11, item 4a)
649-2	Receipts, indices, listings, and accountable records	Destroy after all listed credentials are accounted for. (GRS 11, item 4b)
650	**Visitor Control Files**	
	Registers or logs used to record names of outside contractors, service personnel, visitors, and employees admitted to areas; and reports on automobiles and passengers	
650-1	For areas under maximum security	Destroy 5 years after final entry OR 5 years after date of document, as appropriate (GRS 18, item 17a)
650-2	For other areas	Destroy 2 years after final entry OR 2 years after date of document, as appropriate (GRS 18, item 17b)

Badges are renewed every 5 years for employees and every 2 years for volunteers. Badges issued to contractors expire at end of contract.

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 records disposition schedule above. Obsolete information is deleted at the end of the disposition period. For renewals, outdated information is replaced with current information.

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.

N/A

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

N/A

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

Yes

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. A risk assessment was conducted on August 27, 2007. No risks were identified.

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

Security Control testing was completed on September 2, 2008, using criteria outlined in FIPS 200 and NIST 800-53.

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 11, Credentials and Passes

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

The Privacy Act system of records notice referenced above accurately covers the activities of the Badging and Access 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

See Attached Approval Page

The Following Officials Have Approved this PIA

_____ (Signature) 9/10/08 (Date)

FOR **Kevin McCoy**
Badging & Access System Owner/Manager
8601 Adelphi Rd, Room 2300
College Park, MD 20740-6001
301-837-0298

_____ (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

Martha Morphy (Signature) 9/11/08 (Date)

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