Privacy Impact Assessment (PIA)

Name of Project: LPR Parking Control Ststem

Project's Unique ID: Non-Accessible Stand Alone System

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

Purpose of this System/Application: Control access barriers to satellite parking Archives II, College Park and validate parking authorization at all vehicle entrances of the National Archives in College Park, MD.

Section 1: Information to be Collected

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

Employees		Name, License Plate number, state of registration and affiliation to agency (e.g. contactor, volunteer, another federal agency employees), make of vehicle (e.g. Ford, Toyota, Chevy)
External Users		
Audit trail information (including employee log-in information)		Only security specialist have access with log-ins for this system.
Other (describe)		N/A

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

NARA operational records		Name, License Plate number, state of registration and affiliation to agency
External users		Name, License Plate number, state of registration and affiliation to agency
Employees		Name, License Plate number, state of registration and affiliation to agency
Other Federal agencies (list agency)		The data is not being outside of the physical security office. The only time data would be shared outside of this office is if NARA experienced an event that involved a law enforcement investigation.
State and local		N/A

agencies (list agency)		
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 data element is necessary to identify and ensure indivials are parking in the approved parking areas. Without collected data, the system could not identify if a person should be granted access or not. Visitors and researchers are not in the database an d must show identification before being granted access on to the premises. The sole purpose of the system is to ensure employees and contractors park in their designated areas.

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?
Yes. The system maintains a log of all tags that enter the facility, the time stamp, date/time, the location they entered and left. This is maintained as a 30 day archival file. After 30 days, the data is over written by new information.
There is a camera at the entrance and exit of the Pepco lot and at the main entrance off of Adelphi road.

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 LPR System is controlled in two layers. First the user must log into the specific workstation that is hard wired into the LPR system. This access is via user name and password pairs. Second the user must know a common password to gain access to the information in the system.

NaraNet passwords are not used nor associated with the LPR system. NASS security officials have separate user names and passwords. Passwords are changed on a periodic basis. The Physical Security Team leader determines who has the need for access. There are no log files created.

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. The information in the LPR system can be retrieved by an individual's name and /or vehicle tag number by the system, the state, make of the car or whether the car is identified with a contractor or employee.

9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?
When you search by an individual's name in the database, it is possible to retrieve the license plate number associated with that person. All system users have access to this information.

10. Can the use of the system allow NARA to treat the public, employees or other persons differently? If yes, explain.
Yes. The security guards are given specific post orders that explain how to operate the LPR system and how it distinguishes between employees, contractors and the general public. General public, visitors and researchers will read "Not-in-Database" and will have to show an ID to enter the premises.

For registered vechiles of employees, the screen will read "access granted," while for contractors it will read "Pepco only."

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?
See Section 3 question #1.

13. What controls will be used to prevent unauthorized monitoring?
Authentication to the LPR System is controlled in two layers. First the user must log into the specific workstation that is hard wired into the LPR system. This access is via user name and password pairs. Second the user must know a common password to gain access to the information in the system.

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)?
Rob Wallace.

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?
Employees' data is deleted from the LPR system when they leave the agency. If a security official leaves the division, they will lose login capability of the LPR system.

3. Will users have access to all data on the system or will the user's access be restricted? Explain.
All NASS Physical Security Officials have the same level of access to the LPR system.

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?
Authorized users of the LPR 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.

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? Yes. All necessary software upgrades are done by the contractor with a physical security official present. The contractor brings all software updates to the building and installs them on the server in the SCIF.

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.
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?
The system administrator for the LPR system is responsible for protecting the privacy rights of the public and employees affected by the interface. NARA 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 may result in the employee being unable to park on NARA property.

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 individuals (employee, contractor or volunteer) seeking parking privileges on NARA property. The individual provides vehicle information collection in compliance with NARA notice 2010-060 dated November 13, 2009.

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?
Information is deleted from the LPR System as soon as individuals depart the agency and complete the out processing form NA Form 3009B in compliance with NARA 279 Exit Clearance Procedures for Separating or Reassigned NARA Employees, Contractor Employees, Volunteers, Interns, and Foundation Employees

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.
N/A

The records are not scheduled, no reports are being generated at this time.

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.
The system takes a picture of the physical tag and cross checks with the data in the data base. If the picture matches a tag number in the database then "Access Granted". If the picture does not match any information in the database then it displays "Not-in-Database". For contractors, it may say "Pepco only," indicating they can park in the Pepco satellite lot.

6. How does the use of this technology affect public/employee privacy?
BX will be able to cross check data input (e.g. name and tag number) to a employee or contractors name. Information can be cross referenced in the security access control system or the employee locator on the NARA home page if they have a NARA ID badge or an NARA IT account.

Cross referenced manually

7. Does the system meet both NARA's IT security requirements as well as the procedures required by federal law and policy?
The system continues to be reviewed by the IT security office.

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 in August 2009. No risk were identified.

9. Describe any monitoring, testing, or evaluating done on this system to ensure continued security of information.
System is still under installation phase.
Installation is completed, software is being updated.

10. Identify a point of contact for any additional questions from users regarding the security of the system.
Will Fletcher NASS, All 301-837-1491

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 LPR 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

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)	
Robert Wallace (Signature)	11-10-11 (Date)
Name: Robert Wallace	
Title: Physical Security Specialist	
Contact information: 301-837-3099	
Senior Agency Official for Privacy (or designee)	
(Signature)	11/4/11 (Date)
Name: Gary M. Stern	
Title: General Counsel	
Contact information: 301-837-2024	
Chief Information Officer (or designee)	
(Signature)	11/16/11 (Date)
Name: Michael Wash	
Title: CIO	
Contact information: 301-837-1583	

please provide copies of the PIA to the following:

IT Security Manager
Privacy Act Officer