Privacy Impact Assessment (PIA)

Name of Project: Presidential Libraries Vista Admission System

Project's Unique ID: VISTA

Legal Authority(ies):	**44 U.S.C. 2108, 2111 note, and 2203(f)(1), and NARA 101, Part 4.1**

Purpose of this System/Application:

The system is used to:

- **Facilitate the admission process for visitors to the Presidential Libraries' museums;**
- **Schedule and process individuals and groups for tours, public programs, education programs, etc.;**
- **Manage room reservations, at some Presidential Libraries.**

Section 1: Information to be Collected

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

Employees		The system only maintains information about an employee that is related to his or her duties, including user ID and password. If an employee attends a high-profile event, more infonnation may be collected (see below).
External Users		For groups that interact with each Presidential Library, such as elementary school groups, Boy Scout troops, tour groups, and other groups of people that use the Library, information is stored by group name. An individual (such as a tour leader or a teacher) is assigned to the group. The information collected about this individual is limited to their phone number or email from their place of work. On occasion, such as for events involving VIPs where attendance must be monitored at an individual level, individual information will be collected by the system, including address and telephone number. Credit card information is also collected by the system when used to pay for admission.
Audit trail information (including employee log-in information)		VISTA tracks the usemame of the last user to modify a record as well as the usemame of the user who first created the record.
Other (describe)		VISTA maintains many data elements and fields related to programs and events such as time, location, program type, organization type, event name, resources used, etc.

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

NARA operational records		Libraries will maintain output reports from the VISTA system in conjunction with the reporting requirements of PMRS and of the Data Warehouse.
External users		VISTA processes visitors to the Library. These visitors either walk-up to visit the museum or are scheduled as groups in special events and programs the Library may schedule. Data is input at the time of the walk-up or when a special event, program, or tour is scheduled.
Employees		Information about employees is entered into VISTA as part of a security module that establishes user rights to VISTA. An employee's information might also be entered if he or she participates in a special event.
Other Federal agencies (list agency)		At some Presidential Libraries where we offer combined admittance with a National Park Service (NPS) site, NPS will receive visitor data including attendance and revenue information.
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. VISTA requires basic identification information about visitors, and the Office of Presidential Librares maintains that individuals attending high-profile events should be entered into the system.

2. Is there another source for the data? Explain how that source is or is not used?
There is no other source for data other than what is collected by staff members for walk-up visitation and the scheduling/execution of events.

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?

Through aggregate data compiled in reports, VISTA will assist Library staff members in making determinations about groups that may visit the Library. VISTA also collects ticket type information, so that a Library is able to make determinations about very general demographic information such as numbers of youths, adults, or seniors who visit the Library. No determinations are made based on individual records.

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

VISTA tabulates the number of visitors and how they interact with each Library at the time of the visit and interaction. The data is, therefore, as accurate as possible. Presidential Libraries also maintain paper records related to each event and receipts are maintained for transactions at the admissions desk. This information provides a check on the accuracy of the data in the system.

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

Access to the data is managed by VISTA's security administration module which allows the VISTA administrator to assign user names and temporary passwords (that the user changes upon first login, and then every ninety days as prompted) to every person using the system. These users are organized by groups such as "scheduler" or "front desk staff," and rights are allocated based on these groups. For example, a user who is assigned to the "front desk" group has only limited access to VISTA. She or he can only interact with the point-of-sale admissions portion of the system.

When a user no longer requires access to the system, the VISTA administrator disables that user's account through the VISTA security module.

Additionally, all NARA standards for access to NARANET are applied to ensure protection, and all NARA requirements for systems security have been incorporated.

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

No processes are consolidated, only data consolidated into aggregate totals.

7. Generally, how will the data be retrieved by the user?
Data is retrieved by regular users during the course of their duties. For example, a scheduler of events will often use VISTA to verify the mailing address of a particular group.

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, by name or confirmation number. In most cases, data is retrievable by group name or confirmation number associated with a walk-up visitor transaction or the scheduling of an event. Individual names can be used to retrieve data in the case of group attendance or an individual's participation in a high-profile event.

9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?
With regard to individual information that is captured in VISTA, reports can be produced related to transactions, attendance, confirmation letters, and the nature of the individual's interacfion with the Library. Only confirmation letters will be used in order to allow Presidential Library staff to confirm a group's arrival or an individual's attendance at a high-profile event. Event schedulers and administrators have access to this confirmation-letter report.

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.
VISTA is used to identify individuals who represent groups that have or will visit a Presidential Library. The purpose of idenfifying these individuals is to communicate with them regarding their group's visit to a Library. Data will be maintained in individual records for high-profile events where individual information must be maintained for security purposes.

12. What kinds of information are collected as a function of the monitoring of individuals?
Individuals that are group leaders are identified by name as well as by the phone number and/or email address at their place of business. Individuals participating in a high-profile event are often identified

with this information as well as address.

13. What controls will be used to prevent unauthorized monitoring?
Staff members are only given access to information they will use as part of their duties, per the security module. Moreover, VISTA contains an audit feature that captures user information and the time of any change to the data or the system.

The software is available on authorized staff members' workstations via client technology, and it is password protected both at the VISTA and Novell levels. After fifteen minutes of inactivity the VISTA client locks a user out of the system, and additionally the NARANET workstation will also lock itself after a similar period of inactivity. In both cases the user's password is required to return to an active session in the workstation and in the VISTA client session. Also, the VISTA server is secured in each Library's server room and is also password protected.

All data that is transferred via NARANET is encrypted by VISTA during the transfer.

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)?
Certain Library staff, related to visitor services or scheduling of Library events, have access to the system. Library Directors and their Deputies also have access to the system. In several instances where the Presidential Library works closely with another institution, such as a Library Foundation, staff is given limited access to the VISTA system via dedicated NARA workstations.

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 to the data is managed by VISTA's security module which allows the VISTA administrator at each Library to assign user names and passwords to every person using the software. These users are

organized by groups such as "scheduler" or "front desk staff," and rights are allocated based on these groups. For example, a user who is assigned to the "front desk staff group" has limited access to VISTA. She or he can only interact with the point-of-sale admissions portion of the system. When a staff member no long requires access to VISTA data the local VISTA administrator disables that user account.

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

The level of user access to data is controlled through VISTA's security module. Each user is assigned to a group (administrator, scheduler, front desk staff, etc.) and a user's level of access is determined by the rights assigned to the group to which they belong.

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?

Staff members are only given access to information they will use as part of their duties per the security module. VISTA contains an audit feature that captures user information and the time of any change to the data or the system.

In accordance with NARA policy all users of the system undergo annual training in protecting personally identifiable information (PII) and have acknowledged their responsibilities as they relate to the protection of PII.

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?

Ticketmaster is the contractor for the VISTA system, and Ticketmaster representatives have been involved in configuring the VISTA systems at each Presidential Library.
These actions involved little to no contact with actual data. On occasion Ticketmaster becomes involved in the maintenance of the system. These actions also involve little to no interaction with a Library's data. Nevertheless, the contracts by which Ticketmaster provides service and support for VISTA stipulate that the data is owned by NARA and may not be used in any way by Ticketmaster.

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?
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.
At the Franklin D. Roosevelt Presidential Library (LP-FDR), the National Park Service will have access to reports generated by the VISTA system as part of the close working relationship between the Library and the Roosevelt-Vanderbilt National Historic Sites. Ultimately, proper distribution and use of the data generated by LP-FDR's VISTA system is the responsibility of Library management, specifically the Acting Director.

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 refuse to provide information at any time. A Library staff member may need to inform the individual about how this may affect their reservation to a group or special event (e.g., without a point of contact the Library may not be able to send a letter confirming the group's forthcoming participation in a public event).

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.).

Each Library has a general data policy which guides users in how to input information. These data policies are informed by the VISTA User Guide and by NL Memo 07-36, Reporting Visitation in VISTA. Part of the Office of Presidential Libraries' program review process is a review of a Library's VISTA database to ensure that information is entered in a uniform manner and to ensure that events recorded by VISTA are given some kind of disposition (e.g., completed, canceled, no-show, etc.).

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?

Presidential Libraries offer a host of different public and education programs, price points for walk-up sales, and other events. VISTA was implemented in order to facilitate these processes for each Library. Additionally each Library has generally similar, but often unique business needs supported by the VISTA system. The Office of Presidential Libraries requires that all attendance information be entered into VISTA as defined by NL 07-36, Reporting Visitation in VISTA. This data is reviewed by the Office of Presidential Libraries during site visits, during program reviews, and soon with the assistance of the data warehouse feature.

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

In the records schedule for VISTA drafted with NARA's Records Management Staff all of the data maintained in the system was deemed temporary. The proposed retention periods are either delete/destroy when no longer needed for reference or delete/destroy when the VISTA system is retired.

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.

All reports have been maintained in VISTA to date in support of ongoing business requirements. While the VISTA records schedule does not provide disposal authority for credit card data, the upgraded version of VISTA deployed in the Libraries in FY 2010 (VISTA 6.0) complies with the Payment Application Data Security Standard (PA-DSS) by providing the ability to purge credit card data in accordance with NARA's retention policy for credit card data. The Office of Presidential Libraries will enact the purging policy by providing documentation for VISTA users with administrative rights at each Library to use in carrying out the purges and will ensure compliance with the policy through communication with the Libraries as well as through reviews conducted during formal program reviews and in other site visits.

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?

N/A

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

VISTA was implemented and is operated in accordance with NARA's IT security requirements and all applicable federal laws and policies. VISTA has been certified through the Certification and Accreditation (C&A) process ("VISTA Certification Results" - March 10. 2005). As examples of our continuing compliance with NARA's requirements we are working with NARA's IT Security Staff to update the VISTA System Security Plan (SSP). Contingency Plan (CP). and CP Test Cases.

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?

A risk assessment for VISTA was completed in 2005. and VISTA was considered to operate at a Medium-Low level of risk. The system configuration failures identified during the assessment were corrected

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

The VISTA servers and associated workstations are all within the firewall of NARANET network environment. Additionally, NARA's IT services staff ensure that the antivirus software used to protect the network remains current and that all operating system and other network-related software remain updated. The Office of Presidential Libraries works with NARA's IT Security Staff to support ongoing vulnerability scans and any othe testing needed as part of ongoing certification and accreditation (C&A) of VISTA.

10. Identify a point of contact for any additional questions from users regarding the security of the system.
Sam McClure (LP), 301-837-1958, sam.mcclure@nara.gov

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.
NARA 39, Visitor Ticketing Application (VISTA) Files.

2. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.
No. No modifications of the system would expand the routine uses of records maintained in the VISTA (including categories of users and the purposes of such uses) beyond the uses described in the current Privacy Act system of records notice.

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)	
Sam McClure (Signature)	9/7/2012 (Date)
Name: Sam McClure	
Title: ERA Life Cycle Officer	
Contact information: 8601 Adelphi Road, Suite 2200F, College Park, MD 20740 301-837-1958	
Senior Agency Official for Privacy (or designee)	
(Signature)	9/12/12 (Date)
Name: Gary M Stern	
Title: SAOP and General Counsel	
Contact information: NARA,8601 Adelphi Road, Suite 3110, College Park, MD 20740 301-837-3026	
Chief Information Officer (or designee)	
(Signature)	9.12.12 (Date)
Name: Michael Wash	
Title CIO	
Contact information: NARA,8601 Adelphi Road, Suite 4400, College Park, MD 20740 301-837-1992	