Privacy Impact Assessment (PIA)

Name of Project: Presidential Libraries Visitor Services System (VSS)

Project's Unique ID: VSS

Legal Authority(ies):	**44 USC 2112**

Purpose of this System/Application:

The system is used to:

- Facilitate the admissions process of visitors to the Presidential Libraries and Museums (hereinafter called Presidential Libraries, libraries or library), including online ticketing
- Schedule and process individuals and groups for tours, public programs, education programs, etc.
- Manage room and equipment reservations, for some 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 information may be collected (see below).
External Users		Information is stored by group name 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. An individual, such as a tour group leader, an educator or a member of the public may provide information when registering for events or tours. Registration could take place over the phone, via email, mail, fax or online registration. The information collected about this individual is limited to their phone number or email. 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 mailing address, email 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)		VSS tracks the employee username, date and time of the last user to modify a record as well as the username, date and time of the user who first created the record. User accounts are authenticated via LDAP.
Other (describe)		VSS 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		VSS is replacing a previous system used by many libraries to collect admissions, VISTA. VISTA's data was reviewed and relevant data imported into to VSS for continued use by the library. That data included first name, last name, email address and, in cases of high profile events, mailing address and telephone number. VSS does not rely on other operational records for data.
External users		VSS processes visitors to the Library. These visitors may purchase tickets at the admissions desk and online, and, in some Libraries, at kiosks. Some visitors may be scheduled in groups for tours, special events or programs the Library may schedule. Data is input at the time of the event reservation/purchase. For online reservations, data is input by the visitor(s) and for reservations taken over the phone, via fax or email, NARA staff enters the information.
Employees		Information about employees is entered into VSS as part the Role Based Access Control (RBAC), a security module that establishes user rights to VSS. An employee's information might also be entered if he or she participates in a special event.
Other Federal agencies (list agency)		The FDR presidential library offers combined admittance with a National Park Service (NPS) site. NPS will receive visitor data including attendance and revenue information for that library.
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. VSS requires basic identification information about visitors and the Office Presidential Libraries 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?**
No. There is no other source for data other than what is collected via the VSS at the admissions desk, kiosk or online 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?
Through aggregate data compiled in reports, VSS will assist Library staff members in making determinations about groups that may wish to visit the Library. VSS also collects ticket type information, so that a Library is able to make determinations about general demographic information such as the number of youth, adults or seniors who visit the Library. If there is a credit card payment, then zip code of the customer is collected. This information may be used to communicate future programs and other events that customers may be interested in.

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, VSS will assist Library staff members in making determinations about groups that may visit the Library. VSS also collects ticket type information, so that a Library is able to make determinations about very general demographic information such as the number of youths, adults or seniors who visit the Library. If there is a credit card payment, then zip code of the customer is collected. This information may be used to communicate future programs and other events that customers may be interested in.

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

VSS tabulates the number of visitors and how they interact with each Library at the time of the visit and interaction. Visitors provide their own information when purchasing tickets online or at kiosks. 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, online or at kiosks. 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?

ACME implements access control policies and technical controls to limit access based on least privileges and role based access control to enforce policies around separation of duties. This is audited for PCI compliance and meets requirements 7.1, 7.2, and 8. Policies and processes are in place that require written requests for access and approval from authorized personnel.

(1) ACME explicitly authorizes access through documented access requests and approvals before access is provisioned. System administrators will not provision access without documented request, confirmation of business need for access, and additional approvals beyond the system owner where appropriate. All requests are documented and tracked through closure.

(2) ACME authorized users are instructed in the Information Security Policy and in the Security Awareness Training to only use their specific assigned account, so any actions taken by that account may be tracked.

All VSS users must be ‘onboarded’ via an email invite. This creates an account in VSS that will be sync’d to NARANet’s LDAP info on reply to invite. VSS allows for User account disabling.

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 being consolidated, only data consolidated into aggregate totals.

7. **Generally, how will the data be retrieved by the user?**

a. Data is retrieved by Library staff during the course of their duties. For example, an events scheduler will often use the VSS to verify the mailing address of a particular group.
b. Customers can create accounts to enable them to retrieve information about their purchase.

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, email address, account login, transaction number, Ticket UUID or credit card number

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 can be produced related to transactions, attendance at events, and email correspondence confirming reservations or responding to inquiries. Confirmation emails will be used to allow Presidential Library staff to confirm a group's arrival or an individual's attendance at an event. Event schedulers and administrators have access to this confirmation email 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.

VSS will collect the following information during transactions either at the point of sale terminal, via the phone or email, or from online ticketing and event registration: Name, email, telephone number and/or zip code.

VSS will be used to identify individuals who represent groups that visit a Presidential Library. The purpose of identifying these individuals is to communicate with them regarding their group's visit to a Library. Information is collected in-person, via email or telephone depending on how the individual representing the group contacts NARA.

Also, VSS will collect individuals' name, mailing address, email address, telephone number and zip code when such information must be maintained for security purposes, such as for high-profile events.

12. What kinds of information are collected as a function of the monitoring of individuals?
Group leaders and individuals registering for events online are identified by name as well as by the phone number and/or email address. Individuals participating in a high-profile event are often identified with the same information as well as mailing address.

13. What controls will be used to prevent unauthorized monitoring?
Staff members' access will be limited by rights granted to them via roles in the Role Based Access Control (RBAC) security module. Moreover, VSS contains an audit feature that captures user information and the time of any change to the data or the system.

14. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?
Emails sent through VSS may include web beacons in HTML-formatted e-mail messages that NARA, or its agents, sends in order to determine which e-mail messages were opened and to note whether a message was acted upon or successfully delivered.

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 or the National Park Service, staff is given limited access to the VSS via role-based logins that limit access to certain 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.). Are safeguards in place to terminate access to the data by the user?

ACME has out-of-the-box interfaces with SendGrid and Magtek. These are not persistent connections and are invoked as needed either when sending out emails or when a payment card is being used. VSS also has two additional project specific integrations:

1. With NARA's Novell eDirectory LDAP services (for user authentication), this is not a persistent connection either and is used to validate the user for logins/re-login after timeouts.
2. With NARA Great Plains for posting the financial transactions from ticketing system into NARA's financial accounting system (Great Plains). This is not a persistent connection either and is used for transmitting data from ACME system to NARA's Great Plains MSMQ queue at specified times on daily basis.

The VSS Administrator at each Library determines levels of access to the data. The VSS Administrator controls this by assigning access rights in the VSS's Role Based Access Control (RBAC) security module (AC-6). Roles and Permissions are read-only. For example, a user who is assigned to the "front-desk staff" (FDS) has limited access to VSS. She or he can only interact with the point-of-sale admissions portion of the system (POS) and the reports module of the backend system. When a staff member no longer requires access to the VSS data, the VSS administrator disables that user's account.

Policy for access control is contained within the Security Policies document, which is a part of the NARA IT Security Architecture under NARA Directive 804. The NARA IT Security Architecture contains a supporting document titled NARA IT Security Methodology for Access Control. This document provides guidelines on procedures for implementing access controls within IT systems, and assigns roles and responsibilities for controls within this family. The related controls are documented in the SSP, under AC-1, AC-2.

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 the VSS's Role Based Access Control (RBAC) security module. Each user is assigned a role (administrator, scheduler, front desk staff, etc.), and a user's level of access is determined by the rights allocated to the role assigned to that user.

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?

a. Staff are only given access to information they will use as part of their duties per the RBAC security module. The VSS contains an audit feature that captures user information, when the user logs in and out and the time of any change to the data or the system.

b. 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?

a. Yes. ACME Technologies is the contractor for the VSS and are involved in configuring the VSS at each Presidential Library.
b. Privacy Act clauses are included in the contract with ACME Technologies, including the Addenda to FAR Clause 52.212-4 and FedRAMP Terms and Conditions for Hosted Solutions and Cloud Computing Services.

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.

Yes. The system shares user information with NARA's Novell eDirectory LDAP services (for user authentication). This not a persistent connection and is used to validate the user for logins/re-login after timeouts. integrates with NARA's directory service to validate the users.

The system also provides daily sales and payment totals to the Trust Fund system, Order Fulfillment and Accounting System (OFAS), for reporting and reconciliation purposes.

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

Yes. NARA's directory service is covered by NARANet's PIA and security certification. OFAS also has an approved security certification and PIA.

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

The VSS system owner in conjunction with NARA's General Counsel and Information Security.

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 VSS 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 VSS system is the responsibility of Library management, specifically the Library Director.

Limited financial information is transmitted to the Bureau of Fiscal Service (BFS). BFS provides extended accounting functionality to the agency and serves as NARA's cross-service accounting provider.

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 paying cash at the admissions desk will have the opportunity to decline offering information. Individuals paying by check or credit card share personal information via the method of payment.

Any advanced registration recorded in the system must contain first name, last name, email address and/or zip code when purchasing event tickets online

For online ticket sales and free event registration, mandatory fields will be marked. The individual may decline offering non-required information by skipping those fields. Orders without the mandatory information will not be fulfilled.

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 VSS User and is verified during regular NARA Office Presidential Libraries program reviews of each Library. For the public, accuracy of data is only insured for those paying by credit card or check. Accuracy of credit card information is established by credit card approval. Accuracy of payments by check is insured by comparing information on a check with a customer's government-issued ID (e.g. driver license).

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 system is a single application hosted in the cloud. The required database fields are the same across all Libraries. Data for each site is maintained in a separate environment on the cloud-hosted system and Library users will only have access to their Library's information, and according to the rights granted for their roles. The National VSS Coordinator and the Office of Presidential Libraries will have access to data across the Libraries. This data is reviewed by the Office of Presidential Libraries during site visits, during program reviews and via permissions-based access to the data in the cloud.

3. What are the retention periods of data in this system?
Records are retained and disposed in accordance with records disposition schedules N1-064-08-9 and N1-064-09-5, approved by the National Archives and Records Administration. Museum admission, and facility rental payment records are not included in the above schedules; rather they are covered by the General Records Schedule (GRS) 1.1.

N1-064-09-5
http://www.archives.gov/records-mgmt/rcs/schedules/independent-agencies/rg-0064/n1-064-09-

005_sf115.pdf

N1-064-08-9
http://www.archives.gov/records-mgmt/rcs/schedules/independent-agencies/rg-0064/n1-064-08-009_sf115.pdf

GRS 1.1 Financial Management and Reporting Records
http://www.archives.gov/records-mgmt/grs/grs01-1.pdf

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.

VSS records are covered by N1-064-08-9, N1-064-09-5 and GRS 1.1. However, there vendor keeps data in perpetuity. NARA is working with the vendor to address this issue.

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.

This system offers online ticket purchase and event registration capability and delivery of tickets via email. The service is provided to ACME Technologies by Sendgrid.

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

The new system features, including online advance ticket purchases and event registration, result in NARA collecting additional information about visitors that is necessary to process credit card payments. This information is secured, as described above. The new system will also allow NARA to have additional insights into visitor data at libraries, which will enable better long term planning. Where appropriate NARA's and ACME's privacy policies are linked from each web page.

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

Yes, the system meets these requirements and received an Authority to Operate.

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 performed. A key unresolved risk was the lack of an Account Management Standard Operating Procedure (SOP) for use by Presidential Library Venue Administrators. The SOP should be developed by NARA to include the following:

a. A description of the procedures involved in activating/deactivating a user within the VSS

application.
b. A description of the User Groups available within VSS and what roles are assigned to those user groups and what permissions are associated with those roles.
c. Identify who authorizes the VSS Venue Administrator to activate/deactivate a user within the VSS application including how the VSS Venue Administrator is notified that access for a particular user is no longer needed.
d. Identify who is responsible for reviewing VSS access and monitoring its use as well as the frequency of these reviews.

This will be developed by 4/30/17.

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

The Office of Presidential Libraries works with NARA's IT Security Staff to support ongoing vulnerability scans and any testing needed as part of ongoing certification and accreditation (C&A) of VSS, including updates to the operating system. The environment is scanned on a daily basis for vulnerabilities. When vulnerabilities are identified, an alert is sent to review the vulnerability and take appropriate action. These tools automate parts of the vulnerability management process by using standards for enumerating platforms, software flaws, improper configurations, and measuring vulnerability impact. Identified vulnerabilities are assessed based on impact and risk. Identified vulnerabilities that require action are tracked in a ticketing system through resolution. High or critical vulnerabilities are addressed within 30 days of identification.

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

a. Mary Knill, System Owner

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 Service System

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

Yes, the Privacy Act system of records notice will be updated as the new system is rolled out to ensure it is accurate.

Conclusions and Analysis

1. Did any pertinent issues arise during the drafting of this Assessment?

Yes, questions arose about the vendor’s ability to dispose of information at the end of the contract. NARA is continuing work on this issue. Questions also arose about process by which emails are transmitted to customers and what tracking beacons may be embedded in the email.

2. If so, what changes were made to the system/application to compensate?

NARA worked with the vendor to ensure there is a way to disable beacons in the email communications.

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)	▨
Mary K Knill (Signature)	10/24/17 (Date)
Name: Mary Knill	
Title: Digitization and IT Coordinator for Office of Presidential Libraries	
Contact information: mary.knill@nara.gov	
	▨
Senior Agency Official for Privacy (or designee)	▨
(Signature)	10/23/17 (Date)
Name: Gary Stern	
Title: General Counsel	
Contact information: garym.stern@nara.gov	
	▨
Chief Information Officer (or designee)	▨
(Signature)	(Date)
Name: Swarnali Haldar	
Title: Information Services Executive/Chief Information Officer (CIO)	
Contact information: swarnali.haldar@nara.gov	