Privacy Impact Assessment (PIA)

Name of Project: Presidential Electronic Records Library

Project's Unique ID: PERL

Legal Authority(ies):	The Presidential records in the PERL system entered the legal and physical custody of the Archivist of the United States under the provisions of the Presidential Records Act (PRA), 44 USC 2201-2207. The Act authorizes the normal archival work associated with processing the records and establishes the statutory framework under which these records are accessed.

Purpose of this System/Application:

The Presidential Electronic Records Library (PERL) is a system that contains archival, historical records of the Reagan, George H.W. Bush, and Clinton Presidential administrations. These records are in NARA's legal and physical custody as per the provisions of the Presidential Records Act (PRA). PERL contains distinct datasets of historical records. The bulk of the records in the system are from the Clinton Administration. The purpose of PERL is to allow search and retrieval of these historical records for archival processing, access requests, and reference. This assessment covers both the classified and unclassified versions of PERL.

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 The datasets in PERL are static, historical, archival records received from Presidential administrations.
External Users		N/A The datasets in PERL are for use only by NARA archival staff.
Audit trail information (including employee log-in information)		PERL does contain audit trail information, but that is only available to the system administrators and not to the local users.
Other (describe)		N/A

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

NARA operational records		N/A: Because the datasets comprising PERL are historical records, NARA does not change or alter the information in them. The record information as created and used by the White House came from a variety of sources throughout the given Presidential administration. The only data added to the system, which we term "user-created metadata", is information about the processing status of an individual record. That is, the archival users can record releasability decisions that reside in the system along with the historical, archival records. This functionality is only available in the unclassified instance of PERL.
External users		N/A See above
Employees		N/A See above
Other Federal agencies (list agency)		N/A See above
State and local agencies (list agency)		N/A See above
Other third party source		N/A See above

Section 2: Why the Information is Being Collected

1. Is each data element required for the business purpose of the system? Explain.
The records in PERL are required for the business of NARA and the Presidential Libraries.

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?
The system does not derive data.

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?
N/A

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?
While there is no data being consolidated, the system has controls established by NARA through its IT security requirements. Additionally, there are restrictions under the Presidential Records Act to protect records the disclosure of which would cause a clearly unwarranted invasion of personal privacy.

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.

7. Generally, how will the data be retrieved by the user?
Users (NARA archivists) have the ability to extract data as they perform their archival work. Any privacy data is only retrieved from the system within the context of retrieving archival records in order to answer access requests (either special access or FOIA requests under the provisions of the PRA). Depending upon which component dataset of PERL is being queried, there is either a lesser or greater likelihood of privacy information appearing in the query results. For example, if the Automated Records Management System (ARMS) for email is being accessed, the privacy data is scattered as it would be in any large email system. If the Worker and Visitor Entrance System (WAVES) (White House visits) is being accessed, the results logically contain privacy data. Privacy information, such as social security numbers and medical information, is redacted before any Presidential records are released to the general public.

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.
There is full-text retrieval capability for most of the datasets in PERL. Therefore, if the archivist performing the query knows the name or unique identifier, and that data exists in the system, then

information could be retrieved. Any retrieval of data is not to identify or locate privacy information per se, but is conducted for NARA's archival business and is not for the purposes of identifying individuals other than within the context of legitimate requests for archival, historical records.

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 kinds of reports that could be generated would depend on the dataset and the original application. However, even in the course of archival processing, it would be rare to generate reports from historical records. Any use would be in the context of normal archival processing and the answering of legitimate access requests.

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.
No.

12. What kinds of information are collected as a function of the monitoring of individuals?
There is no monitoring of individuals.

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

14. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?
There are no public web visitors. Authorized staff has access through a web application. PERL login is separate and in addition to the user's NARANet login. NARA implemented the Dynamic Host

Configuration Protocol (DHCP) instead of static IP addresses on the PERL system in February 2011. Each Library user group is assigned to a range of unique IP addresses. Each user within the Library group has his or her MAC or desktop PC address registered with the IT support services, and be added to this specific range of unique IP addresses. To be able to reach to the PERL login page, the Library user must have both a registered address and be with the range of registered IPs for the PERL group. In addition, the user must have the valid authorized user name and password to gain access to the PERL system.

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)?

Archivists and the contract staff responsible for the creation and maintenance of the system have access to the 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?

Archivists use the system to conduct their normal work of archival processing and answering requests under the statutory requirements governing Presidential records. Authorized users log in to the system according to their assigned tasks and business needs. Library archival staff members are only authorized access into the records created by their individual Presidential administration.

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

Users (archivists) at the three Presidential Libraries and at the NARA Presidential Materials Division have access to the datasets necessary for the conduct of their archival business. The product owner establishes and approves access rights within the 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?

There is no unauthorized browsing of data. If access is authorized to the dataset(s) on PERL, then the archivist is performing his or her normal work. A given archivist has access, as approved by the system owner and implemented by the technical support staff, to the datasets for his or her specific Library. The users at the Presidential Materials Division have access to all the datasets across the

Libraries.

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, contractors have developed and maintained the system. Their interactions with any data are covered by non-disclosure agreements. IS has documentation of the contract parameters. However, since these are archival records the provisions of the Privacy Act do not apply.

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?
Archivists redact privacy information before any Presidential records are opened to the public for research.

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?

N/A. These are historical records and no new information is being provided to NARA.

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.).

The data was verified as it was uploaded into the system. There is no issue of "currency" with these historical records, as there is a presumption that the records are accurate and complete at the time of transfer.

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 unclassified system is operated in and maintained at Archives II and is accessed by the appropriate Presidential Libraries (Reagan, Bush, Clinton and the Presidential Materials Division). The classified, non-networked and completely stand-alone, version of PERL is located in a SCIF at Archives I with a clone in the SCIF at the Clinton Library (a duplicate system that also stands alone and is non-networked).

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

Permament. The records in PERL are historical valuable. Should a decision ever be made to propose a subset of these records for disposal, that disposal could only be done in accordance with the provisions of the Presidential Records Act and NARA's Disposal Guidance for Presidential Records.

The "user-created metadata" about releasability has the following retention: Retain metadata for a minimum of 6 years after creation. Then delete when no longer needed for administrative, legal, audit, or other operational purposes

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.

Any disposal of Presidential records would ensure that any information would be destroyed, i.e, degaussed, or burned in accordance with the guidance established for the destruction of electronic records.

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?

Technology used in PERL does not affect public/employee privacy.

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?

No risks regarding safeguarding data in PERL were identified.

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

The primary method to ensure continued security of the information is to view server logs to identify

any unauthorized access. The database server is also continually monitored utilizing both manual and automated intrusion detection softward (IDS). In addition, granular level logging is available but is only activated based on need to evaluate suspicious behavior.

10. Identify a point of contact for any additional questions from users regarding the security of the system.
Tom McAndrew, ISSP, AII, 301-837-1955

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.
N/A. The records in PERL are archival records; therefore the provisions of the Privacy Act do not apply.

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

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.

<u>See Attached Approval Page</u>

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)	(Date)

Name: Kathleen Dillon McClure

Title: Archivist, Presidential Materials Division
       PERL System Owner

Contact information: 700 Pennsylvania Ave., NW, Rm. G-7,
                     Washington, DC 20408-0001
                     202-357-5091

Senior Agency Official for Privacy (or designee)

(Signature)	(Date)

Name: Gary M. Stern

Title: General Counsel / Senior Agency Official for Privacy

Contact information: 8601 Adelphi Road, Room 3110
                     College Park, MD 20740-6001
                     301-837-3026

Chief Information Officer (or designee)

(Signature)	(Date)

Name: Swarnali Haldar

Title: Chief Information Officer

Contact information: 8601 Adelphi Road, Room 4415
                     College Park, MD 20740-6001
                     301-837-1583

The Following Officials Have Approved this PIA	
System Manager (Project Manager)	
[signature] (Signature)	9/12/2014 (Date)
Name: Kathleen Dillon McClure	
Title: Archivist, Presidential Materials Division PERL System Owner	
Contact information: 700 Pennsylvania Ave., NW, Rm. G-7, Washington, DC 20408-0001 202-357-5091	
Senior Agency Official for Privacy (or designee)	
[signature] (Signature)	9/15/14 (Date)
Name: Gary M. Stern	
Title: General Counsel / Senior Agency Official for Privacy	
Contact information: 8601 Adelphi Road, Room 3110 College Park, MD 20740-6001 301-837-3026	
Chief Information Officer (or designee)	
[signature] (Signature)	9/17/14 (Date)
Name: Swarnali Haldar	
Title: Chief Information Officer	
Contact information: 8601 Adelphi Road, Room 4415 College Park, MD 20740-6001 301-837-1583	