Privacy Impact Assessment

Name of Project: Presidential Libraries Museum Collections Management Database – TMS® (The Museum System)

Project's Unique ID: MCMD-TMS

Legal Authority(ies): 44 U.S.C 2108. 2109. 2111. and 2112; also NARA 101. Part 4.2.e.

Purpose of this System/Application: Presidential Libraries (LP) and the Presidential Materials Division (LM) use Gallery Systems COTS application TMS® to document and manage their museum/artifact collections in a systematic manner. Each organization creates and manages data about its own unique collections and business transactions in a dedicated TMS database The Office of Presidential Libraries maintains a Master Catalog with selected. aggregate data drawn from all Libraries' TMS databases. TMS is hosted and managed by vendor Gallery Systems within a government only cloud computing environment that is FISMA-compliant.

Section 1: Information to be Collected

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

a. **E**mployees. Employee names may appear in TMS 'Constituents' (name authority) records and are linked to object records according to various daily collections management roles such as 'curator', 'cataloger', 'approver' or 'handler'. No additional information is recorded about constituents acting in these capacities

An employee may occasionally be associated with a collection in the capacity of a collection 'donor', 'gifter' (the individual gave Presidential gift which is now part of the collection), 'depositor' (donation pending), lender, or 'maker' (the individual crafted or authored a collection artifact). An employee's personal street address and/or birth/death dates may be recorded in the system in connection with these roles.

b. **External Users:** N/A

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

User logins and system privileges are assigned to employees with a need to access to the TMS system. Logins and security settings are managed by the TMS System Administrators. Requests to add, modify or remove user names and rights are provided to the Administrators on a written request form by an authorized individual at each Library User request forms are archived and linked to the TMS system as media records and retained permanently, accessible only to individuals with System Administrator privileges. The system does not internally archive user names or privileges that have been removed.

Within the application. TMS tracks the username of the last user to modify a record as well as the username of the user who first created the record. TMS also tracks all changes made in core data fields. For Constituents. these fields include· Display Name. Display Date. Institution. Nationality. Culture; status flags (checked or unchecked) designating if the Constituent record is Active, Approved. is a 'Private Collector'. and

Public Access (the Constituent record (designated data fields only) may be made available for public access (via web interface). Constituent contact information and birth/death dates are not captured in an audit trail

d. Other (describe) TMS functions as a descriptive catalog of the museum collection, and supports a full range of collections management processes (acquisitions, cataloging, de-accessions, location and movement, condition, loans and exhibitions). TMS organizes this information within the following, interlinked modules:

- Objects Catalog: comprehensive descriptive, historic and tracking information for objects in the collection
- Constituents: (name) authority records which record background and/or contact information for individuals or organizations with a specified role(s) in relation to the collections or to collections management processes, i e. Donor, Gifter, Conservator, Borrower/Lender, etc., associated with the collections.
- Media module: physical and descriptive metadata for media files that are associated with TMS and may be linked to records throughout the database
- Loans and Exhibitions
- Sites: authority records which record background information for geographical sites with historic or other relationship to the collection
- Events: authority records which record background information for events with historic or other relationship to the collection
- Publications – citations for books, web, and other published materials with collection item citations
- Thesaurus: controls multiple thesauri and other keyword associations that may be utilized within TMS modules

Individual records within all modules may be interlinked as needed

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

a. NARA operational records: information for loans and exhibitions may be obtained from and are redundant to a Library's museum operational records for acquisitions, deaccessions, transfer/shipment, loan and exhibition files

b. External users: N/A

c. Employees: See I.a above: an employee's personal contact information may be included in the system if the individual has acted as a collection donor, gifter, depositor, lender, or maker This information is 1) obtained through personal contact/inquiry by collections staff interacting with the individual, for example in the course of completing a deed of gift or a loan agreement; or 2) as part the information received with White House gift records An individuaFs birth/death dates may be included in the system if he/she has acted as a collection gifter or maker. Birth and death date information is obtained by collections staff from public sources (Who's Who (print), CIA World FactBook (web), etc).

d. Other Federal agencies (list agency). The Presidential Materials Division (LM) manages and stores material on courtesy storage for the White House Data for Presidential Gifts that come to NARA for courtesy storage is imported from incumbent White House Gift Office.

This includes baseline descriptive and tracking information about gifts that NARA has received for courtesy storage, and information about individuals who gave (and possibly also crafted or authored) a gift. Such information might include the individuaFs street address, institutional affiliation, and title, and when/how the gift was acknowledged

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

f. Other third party source: Entries into the system are directly composed into the system based on records and processes accompanying or created in the course of acquiring, cataloging and managing the objects. This information is obtained through 1) information recorded by the White House in the form of White House Gift Office records and inherited by NARA as record holdings, and/or 2) personal contact/inquiry of collections staff interacting with the individual, for example in the course of completing a deed of gift or a loan agreement, and/or research in published print or web sources (e.g. Who's Who, CIA World FactBook)

Section 2: Why the Information is Being Collected

1. Is each data element required for the business purpose of the system? Explain.

Yes.

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

Yes The Presidential Libraries maintain internally-generated textual collections management records as well as archived records from the White House Gift Office. Information in TMS is obtained through 1) information recorded by the White House in the form of White House Gift Office records and inherited by NARA as record holdings; and/or 2) personal contact/inquiry of collections staff interacting with the individual, for example in the course of completing a deed of gift or a loan agreement; and/or research in published print or web sources (e.g. Who's Who, CIA World FactBook)

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?

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?

Passwords and usernames are required to access the system. System users are validated and have specific permissions commensurate with their job responsibilities to access the TMS system, and to access specific TMS data fields.

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?

At the individual workstation, the system has search and browse functions for retrieving and reporting data. Individuals may only browse, retrieve and report information according to the privileges assigned to their login.

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.

Data pertaining to an individual is retrievable by a unique entry of the donor's name or other textual elements in the Constituent records, e.g alternate names, title or occupation, city/country and other address or biographical elements No information is entered or retained in TMS for individual SSN or other personal identifiers.

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 might include lists of artifacts an individual gave as a gift to a President or other recipient, or items the individual has deposited, donated or loaned to the Library. Reports, forms and correspondence may be generated in connection with the completion of deeds of gift, loan agreements, or in connection with professional services for the collection (e g conservation or shipping services). Museum staffs use these reports to manage the artifact collections

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

N/A

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?

N/A

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?

No.

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)?

Access to TMS is limited to TMS users and administrators with a designated need to access the system TMS users include Office of Presidential Libraries and Presidential Libraries museum collections staff, interns and volunteers, and designated Library administrative staff. Specific access rights are assigned according to each individual's assigned tasks to support museum operations All users must have an active NARAnet login.

TMS is hosted and managed by vendor Gallery Systems within a government only cloud computing environment. TMS system administration is managed by a Gallery Systems Base System Administrator, and a NARA Program System Administrator. The Base System Administrator has appropriate clearances commensurate with the vendor contract, and is a badged NARA contractor with a NARAnet login. The Program System Administrator is also the NARA System Owner and ISSO.

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.).

An authorized individual with senior collections management responsibilities at each Library determines what users are to be added to a Library's TMS database and what rights will be assigned commensurate with the user's assigned duties Requests to add, modify or remove user names and rights are provided in writing by the Site Administrator to the Program System Administrator, who vets and approves requests, and coordinates with the Base System Administrator to establish logins and manage security groups Configurations, policy and procedures for TMS security and user settings are documented in the TMS Detailed Design, the TMS System Security Plan, and SOP's for TMS Security and User settings. These SOP's ensure that that accounts are properly disabled when employees change jobs, leave the agency, etc

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

The following security access controls can be managed in TMS as configured by individuals with System Administration rights:

- *Security Groups* Each user is added to a Security Group; this group is then granted *View, Edit, Add,* and *Delete* rights per module/table/field in all modules, throughout the database.
- *Departments*. Users in each Security Group are granted (or denied) access to records assigned to specific Departments which have been established in TMS Objects, Exhibitions, and Loans modules
- *Modules, Tables, and Fields* The four basic security rights which relate to data in modules, tables, and fields in TMS - *View, Edit, Add,* and *Delete* - are granted (or denied) to users in each Security Group.
- *Functions* Users in each Security Group are granted (or denied) the right to perform additional functions Exporting a list to Excel, printing an image, deactivating a move transaction, opening an image in an external viewer, etc
- *Overall* Overall controls access to data via searching, generating reports, the Related menu, blanket security settings for special Security Groups such as *"No Rights"* and *"System Administrator"*

Requests to add, modify or remove user names and rights are provided by each Library's Site Administrator to the TMS Program System Administrator, who vets and approves requests, and coordinates with the Base System Administrator to establish system logins and manage security groups

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)?

System users (NARA staff) are validated and have permissions commensurate with their job responsibilities Users receive systematic training and training materials for TMS under the vendor contract terms with the oversight of the Program System Administrator

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?

The system is fully supported and maintained at the system level by NARA's IT contractor Gallery Systems, Inc., and the Office of Presidential Libraries has a service contract with the vendor. A Privacy Act clause was affixed to the contract In addition, the vendor has signed a Confidentiality Agreement specific to this contract. All individuals with access to NARA data have received NACI clearances Individual vendor employees with a designated need receive a NARA contractor badge and NARAnet login.

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.

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.

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

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 TMS system meets extensive international documentation standards specified in the contract Performance Work Statement ata entry and other manual procedures conducted in the system are controlled by guidelines created and/or maintained in alignment with these standards and additional NARA specifications by the Office of Presidential Libraries Program System Administrator: i.e. a unified TMS Data Dictionary, *Presidential Libraries Guidelines for TMS Data Entry* and data elements standards *(Presidential Libraries Artifact Data Standards Working Guidelines)* maintained in cooperation with NARA's Lifecycle staff. Quality control is conducted at each site by a designated TMS Site Administrator and reviewed under LP management assurance protocols.

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?

All physical and logical management of the TMS application is centralized under the oversight of the contract vendor's Base System Administrator (system level) and the Presidential Libraries TMS Program System Administrator (application level) Local quality control and configuration management at the application level is conducted at each Library by a designated TMS Site Administrator.

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

The artifacts and associated processes documented in TMS are NARA holdings that have been transferred or donated to NARA for permanent retention, on temporary deposit with NARA pending future donation, or on temporary loan for program exhibition/display purposes. Retention of this information is for as long as the system is operational, at which time data is migrated to a superseding system

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.

MCMD is scheduled under NARA files schedules as a Temporary system. Data is updated/overwritten as information is superseded, and deleted when no longer needed for administrative, legal, audit, or other operational purposes.

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?

TMS has a complete NARA System Security Plan on file and is subject to all assessment and testing commensurate with a FISMA Moderate information system. For any requirements determined to be deficient, a mitigation response is developed and tracked through a NARA POAM.

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 full risk assessment for TMS was completed during the development pilot phase prior to receiving Approval to Operate by NARA's CIO, and will be conducted annually going forward For any requirements determined to be deficient, a mitigation response is developed and tracked through a NARA POAM

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

Security testing and assessment commensurate with a FiSMA Moderate system was completed during the development pilot phase, and will be conducted annually going forward For any requirements determined to be deficient, a mitigation response is developed and tracked through a NARA POAM As documented in the TMS SSP, there are several tools used to continuously monitor security-related activity for TMS, such as network and host based intrusion detection, log monitoring through a security information manager (SIM), and other monitoring agents that run on TMS servers.

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

Kim Koons, MCMD-TMS System Owner, ISSO and Program System Administrator,

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 3. Donors of Historical Materials Files.

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

No.

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 Anproved this PIA

(Signature) Jan 22, 2013 (Date)

Kimberly Roons
System Owner, MCMD-TMS
700 Pennsylvania Avenue, NW
Washington, DC
Room B5, A1
202-357-5082

(Signature) 1/25/13 (Date)

Gary M. Stern
Senior Agency Official for Privacy
8601 Adelphi Rd,
College Park, MD
Room 3110
301-837-2024

(Signature) (Date)

Michael Wash
NARA Chief Intormation Officer
8601 Adelphi Rd,
College Park, MD
Room 4400