

Privacy Impact Assessment (PIA)

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: The Office of Presidential Libraries (LP) and the Presidential Materials Division (LM) use Gallery Systems COTS application TMS[®] to document and manage their museum/artifact collections and museum operations in a single repository. Each custodial division creates and manages data about its own collections and museum business transactions in a dedicated TMS database that resides on a centrally-administered and centrally-accessible FISMA-compliant cloud computing environment. TMS is the primary repository for item-level descriptive information about the Presidential Libraries artifact collections, fully integrated with holdings acquisition, provenance, tracking, preservation, exhibit, loan and contextual information, processes and reporting. eMuseum[®] is the web-publishing application for TMS, and allows external visitors to browse and view sharable TMS content without permitting access or writing privileges to the TMS database. eMuseum offers flexible search options, and is also capable supporting API's and other methods for providing programmatic access to collections information.

Section 1: Information to be Collected

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

Employees	<p>1) Employees who are TMS Account-holders: First Name, Last Name, Position/Title, Custodial unit name, user account active dates and user login name recorded in the TMS Constituents module.</p> <p>2) Employees who are Museum account holders: First Name, Last Name, eMuseum username, eMuseum password, and email address recorded in the eMuseum application.</p> <p>3) If an employee is associated with any holdings documented in TMS in an Acquisition-related role (e.g., donor, gifter, depositor) or in an Object-related role (e.g., creator, maker, artist), additional information may be recorded such as their personal street address (Constituents>Address) or other contact information (Phone, email address), general biography (Constituents>Biography), birth/death dates (Constituents>Display Name>Begin date, End date), place of birth or activity (Constituents>Geography>types Place of Birth, Place of Death, Place of Activity), general biography (Constituents>Biography), title (Job Title), alternate names/titles or other biography (Constituents>Alternate names, Alternate bios) and associated topical keyword terms (Constituents>Attributes).</p>
------------------	--

External Users	<p>To the extent that NARA contractors or eMuseum visitors have accounts in TMS, information about them will be the same as for categories 1 and 2 above.</p> <p>To the extent that NARA contractors, eMuseum visitors or other external individuals are associated in an Acquisition-related role (e.g., donor, gifter, depositor) or and Object-related role (e.g., creator, maker, artist), information about them may include the same data elements as indicated for Employees above.</p> <p>Website visitors who sign up for an eMuseum account are asked to provide their first and last name, a user name, and an e-mail address.</p>
Audit trail information (including employee login information)	<p>TMS DATABASE: The TMS audit trail records all changes to salient data fields, including the previous entry, the new entry, the date/time of the change and the user login name that made the change. Optional fields record an explanation and approval for the change.</p> <p>EMUSEUM WEB APPLICATION: there is no independent audit trail in the eMuseum web application.</p>
Other (describe)	
Describe/identify which data elements are obtained from files, databases, individuals, or any other sources?	
NARA operational records	<p>TMS DATABASE: a NARA employee TMS account holder's title/position and dates of service in that position may be obtained from on-site NARA unit personnel records. Contact information for individuals with an acquisition-related or object-related function may be obtained from operational holdings acquisition or loan processing files or transactions.</p> <p>EMUSEUM WEB APPLICATION: no information is obtained from NARA operational records.</p>
External users	<p>TMS DATABASE: Information associated with holdings acquisition or object-related functions may be provided by external users in the course of acquisition, processing, exhibit or loan business functions.</p> <p>EMUSEUM: name, user name and email address</p>
Employees	<p>TMS DATABASE: information about the employee's title and dates of active account use is entered by the system administrator in the authority record for users who have a TMS account.</p> <p>EMUSEUM: name, username and email address</p>
Other Federal agencies (list agency)	<p>Information about individuals associated with collection holdings acquired through the Executive Office of the President (i.e., gifts given to White Office employees during a President's term in office) may be provided by the White House Office of Correspondence records or personnel.</p>
State and local agencies (list agency)	N/A
Other third party source	<p>Information about donors, items or people in the holdings may be obtained from 3rd party sources such as public research catalog authorities, and a variety of published print or web sources (e.g., Who's Who, CIA World FactBook, auction catalogs, creator's websites, etc.).</p>

Section 2: Why the Information is Being Collected

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

TMS DATABASE: All data elements that include personal information support the specific business purposes of the custodial unit, i.e. as a standard component of holdings processing and cataloging processes, and/or MCMD database administration processes.

EMUSEUM WEB APPLICATION: information provided by account holders is strictly voluntary, and obtained for the purpose of account verification and management. Users who create and account receive the ability to use the 'My Collections' function. This function allows the user to save and name queries from application data for later access and voluntary sharing with other application visitors and users. Application administrators may also grant account holders – for example, authorized internal users – higher privileges in the application, for example access to additional descriptive data about the collections, or access to limited application administration functions. eMuseum user accounts do not allow access to the webserver, to background application configuration files or to the TMS data repository.

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?

No - N/A.

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?

TMS: 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 and functions. Each Library site can access its own TMS domain only and cannot access other Library or LM TMS data. The system offers extensive additional controls and task support for protecting constituent records for Donors or other individuals who have requested anonymity as specified in their instrument of gift. Additional item-level and field-level controls can be applied to also applied to any media (documents, images, audiovisual files) linked to collection records.

eMuseum: eMuseum visitors and user-level account holders are only able to access limited information about the artifacts on a read-only basis. Collections information released to eMuseum is a one-way data push from the TMS application, and has been fully vetted and approved for release and allows no writing access to TMS data. Individuals with administrative eMuseum accounts can access a limited eMuseum configuration interface, which allows authorized account-holders to schedule application data refresh, name eMuseum field tags, determine the order that eMuseum data fields are displayed, and perform some limited media administration, such as standardized image sizing, and to view and assign privileges to user accounts. None of these functions in any way affect data or functions in the TMS data repository.

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?

TMS: At the individual workstation, the system has multiple search and browse functions for retrieving and reporting data. Security controls that apply to account users, for example that limit access to certain data fields or functions are automatically applied to all reporting systems. The system supports highly granular data security at many levels and down to the field level to ensure that individual users may only browse, retrieve and report information according to the privileges assigned to their specific user account.

eMuseum: eMuseum offers has search, and browse and filtering functions for retrieving and reporting data for eMuseum visitors and user-level account holders. Visitor who choose to create a user account gain the additional ability to save and name data queries called 'My Collections', and potentially (if permissions are allowed to the user's assigned security group) share their 'collections' with other eMuseum visitors.

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 additional

alternate names, a unique Constituent ID assigned by the system when the record is created. No SSN or other unique personal identifiers are entered.

9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

TMS: Reports can be designed and generated using any field in the database, including information recorded in Constituent authority records. For example, the system can generate a deed of gift or a receipt for holdings that may include an individual's name and street address. A report could be generated that includes an employee's name, NARA title and dates of account use. Museum staffs use these reports to document and research the object collections, and to manage all associated collections management and data administration processes. All access and security controls applied to data fields, functions and media and associated with a user's account automatically apply to all reporting mechanisms in the system.

eMuseum: The system records and can report information about account holders (name, user name and email address), and the name and date of any 'My collections' that are created and any data that is added to 'My Collections' note fields. Authorized application managers will use this data to fulfill monitoring requirements for publically-created content according to NARA policy and procedures. General visitor analytics (i.e., reporting who has visited the website and what visitors are doing) are performed via Google Analytics and Google Tag Manager, which are applied to the system and used according to NARA policy and procedures.

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

The eMuseum application allows application administrators to manage and assign different user groups and associated privileges to those who create a user account. For example, authorized internal NARA users may be allowed access to additional descriptive data in order to perform holdings research to prepare for an exhibit. Authorized staff may be granted access to their home unit's application administration dashboard in order to perform assigned data management duties. The parameters for these user groups are documented in MCMD SOPs.

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.

TMS: The TMS audit trail may be used by program administrators in the Office of Presidential Libraries or a Library's local site administrator to associate employee's user login with application data quality management processes and collections accountability functions such as collection inventories and location and movement controls.

eMuseum: Google Analytics will be used to generate summary statistical data, and will not be used per se to monitor the activity of specific individuals. The activity of individual 'My collections' users will also be used to create summary statistical data, and will also be monitored in order to fulfill NARA

policy and procedures for public content.

12. What kinds of information are collected as a function of the monitoring of individuals?

N/A

TMS: The TMS audit trail allows collections supervisors to monitor and maintain data entry quality control – for example to maintain application data standards, and to support collections accountability functions such as collection inventories and location and movement controls according to employees’ assigned tasks and responsibilities.

eMuseum: Google Analytics data will be used according to NARA policy and procedures to monitor and analyze user interest satisfaction with application data. ‘My collections’ data will be monitored to also analyze user interest and satisfaction with application data, and also to monitor and manage publically-created content according to NARA policy and procedures.

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

Access to TMS audit trail information is restricted to the System Administrator and Library Administrator security groups. Library Administrators have access to their own site’s TMS only. Security group administration is functionally and procedurally limited to the System Administrator security group under established MCMD SOPs. System Administrator access is limited to the MCMD Program System Administrator (currently the Office of Presidential Libraries Museum Collections Officer) and his/her delegates and contract application host personnel assigned to MCMD. All contract individuals have signed non-disclosure agreements and operated under the terms of the hosting contract SOW and SOPs

Access to the eMuseum administrator security group is limited under MCMD SOP’s to the TMS System Administrators and individual site Library Administrators and his/her delegates. eMuseum administrators have physical access only to their own site’s eMuseum.

14. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?

eMuseum stores the user’s session id to a cookie, which expires when the session expires or after 30 minutes of inactivity. Google Analytics will store its own set of cookies which eMuseum does not manage. “Remember me” has been disabled to further reduce the use of cookies.

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)?

TMS: 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 other Library and NARA staff who work with the artifact collections, and host contract staff assigned to NARA's MCMD system. Specific access rights are assigned according to each individual's position responsibilities and assigned tasks regarding collections information. All users must have an active NARAnet login. The system can only be accessed from within NARAnet. Each Library site can access their own TMS database and cannot access other site's TMS database.

eMuseum: any NARAnet user who is aware of the url may access internal eMuseum published data. Access to application administration data is limited to MCMD system administrators (NARA contract and system administrators and contract support). Access to data published from a public instance of eMuseum is open to all internet users. Access to restricted eMuseum data and application configuration functions is limited to MCMD system administrators, contract support staff and Library administrators and his/her delegates, as outlined in MCMD SOP's. Library staff have physical access to their own site's eMuseum only in order to gain and use administrative privileges in eMuseum.

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?

TMS: Each TMS Library Administrator (usually the Library Registrar) coordinates with the individual's supervisor to determine what users are to be added to a TMS database and what data and transactions the user needs access to commensurate with the user's assigned duties. Requests to add, modify or remove user accounts and security group assignments are provided in writing by the TMS Library Administrator to the Program System Administrator (System Owner), who coordinates with the Gallery Systems host administrator/engineer to establish domain level accounts, add/remove logins at the application level, and manage Security group settings. These protocols are codified in MCMD-TMS SOPs.

eMuseum: NARAnet and public internet may access published eMuseum data on a purely voluntary basis, and may elect to create a general user-level account. Only users with a 'superuser' level account may access eMuseum administrative data. When an eMuseum application is implemented, the contractor assigns 'superuser' status to the Program System Administrator (System Owner). The PSA/SO prompts the respective TMS Library Administrator to create a user account, and assigns that individual 'superuser' status, and delegates further account management for that instance of eMuseum to the Library Administrator under the oversight of the PSA/SO according to NARA Policies and Procedures for account management. Protocols for account creation/removal, monitoring and review are codified in eMuseum SOPs and a local eMuseum Content Workflow Management Plan.

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

TMS: Individual users are only allowed access to data fields (specifically, to Add, Edit, View, Delete) to permissions to perform database transactions as commensurate with their assigned duties.

eMuseum: eMuseum visitors have access to all published data on eMuseum. Access to internal-only descriptive information or 'superuser' administrative data is assigned on the basis of the employee's assigned duties.

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?

TMS and eMuseum: System users are validated and only have permissions commensurate with their job responsibilities. Users receive systematic training and training materials under the oversight of the NARA Program System Administrator (System Owner), including vendor-provided training, NARA/LP training, vendor-provided user guides, LP-provided user guides and data standards. Each Library Administrator is delegated responsibility for local TMS and eMuseum quality control and eMuseum account management under the oversight of the Program System Administrator. TMS data and transactions are regularly monitored based on standardized quarterly data development reports submitted by each Library to the Office of Presidential Libraries. Library Directors provide assurance in the Library's annual assurance statement that all TMS users have received instruction regarding the protection of PII and other sensitive data in artifact collection records. In addition, each eMuseum is monitored and controlled under a local Content Workflow Management Plan which is jointly developed and monitored by the Program System Administrator and the Library site administrator in cooperation with the NARA Web Program.

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?

MCMD, including all applications and tools, is a hosted system, i.e., supported and maintained by contractor Gallery Systems, Inc. under a service contract with the Office of Presidential Libraries. A Privacy Act clause was affixed to the contract, and any personnel working directly with the NARA system have signed a non-disclosure Agreement, and are subject to contract requirements. All individuals with access to NARA data have received NACI clearances.

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.

TMS: No.

eMuseum: other agencies will have access to public eMuseum data in the same manner as other public visitors/users.

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?

TMS: N/A

eMuseum: Creating an account on the eMuseum application is entirely voluntary. Account users are informed about the information they provide at the time of account creation.

2. Does the system ensure “due process” by allowing affected parties to respond to any negative determination, prior to final action?

TMS: N/A

eMuseum: Should NARA determine that publically-created content is inappropriate and should be removed from public eMuseum websites, parties will be responded to according to current NARA’s public contribution policy.

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 application meets extensive international standards and NARA requirements specified in the contract Performance Work Statement. All data entry and procedures conducted in the system are controlled by NARA/LP data standards and data entry guides and SOP's maintained by the Office of Presidential Libraries Program System Administrator/System Owner. Responsibilities for local quality control are assigned to a designated TMS Library Administrator at each site and reviewed under the system SOP's and 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 Presidential Libraries TMS Program System Administrator/System Owner (application level), who

develops, disseminates and monitors data entry protocols and compliance. Local quality control is conducted at each Library by a designated TMS Library 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. Data in TMS is updated/overwritten as information is superseded and deleted when no longer needed for administrative, legal audit or operational purposes. The period of retention is "retain as long as administratively needed."

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, and the period of retention is "retain as long as administratively needed." 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.

Access to the TMS system (for authorized users) is commensurate with the same technologies implemented on their NARA workstation and for their NARAnet login.

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?

The MCMD PWS provides for all levels of the system to comply with requirements commensurate with a FISMA Moderate information system as well as NARA enterprise requirements. The MCMD ISSO ensures that current NARA scanning protocols are active and functioning, reviews security scans, and coordinates with the MCMD host vendor and other members of the MCMD OM team to address any POA&Ms and maintains current security documentation.

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?

TMS: A full risk assessment for TMS and public eMuseum was completed during the development pilot phase prior to receiving Approval to Operate by NARA's CIO, to be conducted every 3 years thereafter. A new ISSO was assigned to MCMD under the current information security services contract, and is currently working with the host vendor and other members of the MCMD OM team to update all security protocols, resolve any POA&Ms and ensure that all documentation is current according to NARA and federal requirements.

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

The MCMD ISSO is currently working with the MCMD team to implement monthly security scanning and POA&M resolution. The MCMD SO provides monthly verification/approval of users with administrative privileges. Contingency plan testing is done annually (last completed September 2016).

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

Corey Smith is the MCMD ISSO. Kim Koons, the Presidential Libraries Museum Collections Officer, serves as the MCMD-TMS System Owner 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?

No.

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)

(Signature)

(Date)

Name: Kimberly Koons

Title: Presidential Libraries Museum Collections Officer

Contact information: ARC I
700 Pennsylvania Avenue, NW
Room G-29
Washington, DC
202-357-5082

Senior Agency Official for Privacy (or designee)

(Signature)

12/11/18

(Date)

Name: Gary M. Stern

Title: General Counsel

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

Chief Information Officer (or designee)

(Signature)

12/18/18

(Date)

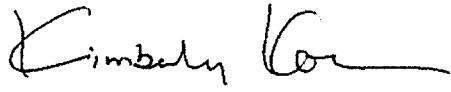
Name: Swarnali Halder

Title: Chief Information Officer

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

The Following Officials Have Approved this PIA

System Manager



Dec 11, 2018
(Signature)

(Date)

Name: Kimberly Koons, System Owner

Title: Presidential Libraries Museum Collections Officer

Contact information: ARC I
700 Pennsylvania Avenue, NW
Room G-29
Washington, DC
202-357-5082

Senior Agency Official for Privacy (or designee)

(Signature)

(Date)

Name: Gary M. Stern

Title: General Counsel

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

Chief Information Officer (or designee)

(Signature)

(Date)

Name: Swarnali Halder

Title: Chief Information Officer

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

