

United States Department of State



**The Museum System (TMS)**

# **Privacy Impact Assessment**

Bureau of Administration

# TMS PIA

## 1. Contact Information

**A/GIS/IPS Director**  
Bureau of Administration  
Global Information Services  
Office of Information Programs and Services

## 2. System Information

- (a) **Name of system:** The Museum System (TMS)
- (b) **Bureau:** OBO
- (c) **System acronym:** TMS
- (d) **iMatrix Asset ID Number:** 458
- (e) **Reason for performing PIA:**
- New system
  - Significant modification to an existing system
  - To update existing PIA for a triennial security reauthorization
- (f) **Explanation of modification (if applicable):** Not applicable.

## 3. General Information

- (a) **Does the system have a completed and submitted Security Categorization Form (SCF)?**  
X Yes \_\_\_ No
- (b) **What is the security Assessment and Authorization (A&A) status of the system?**  
The Department of State operates TMS in accordance with information security requirements and procedures required by federal law and policy to ensure information is appropriately secured. The Department will schedule a risk assessment of the system, and identify appropriate security controls to protect against that risk, and implement the controls. The Department performs monitoring, testing, and evaluation of security controls on a regular basis to ensure that the controls continue to work properly. In accordance with the Federal Information Security Management Act (FISMA) provision for the triennial recertification of this system, TMS has completed the assessment phase of A&A and is currently in the process of being accredited. We anticipate ATO will be granted upon completion and approval of this PIA. TMS is currently going through accreditation.
- (c) **Describe the purpose of the system:**

The Museum System supports Overseas Buildings Operations' mission requirements to manage over 2000 exhibitions. Art in Embassies (AIE) utilizes The Museum System (TMS) database, which is designed specifically for museums, to maintain all aspects of collections management. TMS fully integrates exhibitions, shipments, publication and outreach in one comprehensive database. TMS uses Crystal Reports, which allows customized reports to be written for any need within the curatorial, registrar, or publications departments. The data is used to link the lender contact information to the loaned or purchased artwork. The loaned artwork is returned to the lender at the end of the exhibition; thus the need for address, phone, and email information. The lender's PII is retained in TMS as this tracks all works of art and its constituents. TMS serves as a reference for past loans and purchases. The birth year and headshot of the lender is exported to the website along with the information of the artwork, i.e. (title, dimension, medium). The lender can be a museum, gallery or collector along with the lender. We collect contact information on the lender along with the artwork which they loaned. .

**(d) Describe the PII that the system collects, uses, maintains, or disseminates:**

- a. Lender's name
- b. Lender's birth year (Optional)
- c. Address of business or phone numbers
- d. Lender's photo (Optional)

**(e) What are the specific legal authorities and/or agreements that allow the information to be collected?**

- [22 U.S.C. § 300](#)
- [15 FAM 740 \(Office of Art in Embassies\)](#)
- [15 FAM 773 \(Office of Art in Embassies- Requirements\)](#)
- [2 FAM 962.5 \(Acceptance: Gifts of Artwork\)](#)

**(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?**

Yes  If yes, provide:

- SORN Name and Number: SORN STATE 46, Fine Arts Records
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): September 27, 1977 (State-46 is currently being updated to ensure proper coverage for this PIA. It is expected to be published by July of 2016).

No  If a SORN is not required, explain how the information is retrieved without a personal identifier.

**(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? Yes  No**

If yes, please notify the Privacy Division at [Privacy@state.gov](mailto:Privacy@state.gov).

**(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? Yes  No**

(If uncertain about this question, please contact the Department's Records Officer at [records@state.gov](mailto:records@state.gov) .)

**If yes provide:**

- Schedule number (e.g., (XX-587-XX-XXX)): [A-08-010-05](#)
- Type of information retained in the system: Control Cards maintained by Lender, Country where located, Title and by assigned number.
- Length of time the information is retained in the system: NN-170-140

#### 4. Characterization of the Information

(a) **What entities below are the original sources of the information in the system? Please check all that apply.**

- Members of the Public
- U.S. Government employees/Contractor employees
- Other

(b) **If the system contains Social Security Numbers (SSNs), is the collection necessary?**

Yes \_\_\_ No X (SSNs are not collected)

- If yes, under what authorization?

(c) **How is the information collected?** Information is collected directly from the lender through the Art in Embassies loan agreement or permanent collection documents.

(d) **What process is used to determine if the information is accurate?** Verification from the provider.

(e) **Is the information current? If so, what steps or procedures are taken to ensure it remains current?** Information is current. The lender will contact us in case of information change/and AIE is in contact with lender prior to the return of objects.

(f) **Does the system use information from commercial sources? Is the information publicly available?** Yes, we can retrieve/update information from websites/catalogues, etc. Yes, the information is public.

(g) **Is notice provided to the individual prior to the collection of his or her information?** Yes, the individual is responsible for providing and confirming correct information to AIE, so he/she is aware of the information that will be collected and our purpose for collection.

(h) **Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information?** Yes X No \_\_\_

(i) **How did privacy concerns influence the determination of what information would be collected by the system?** Privacy concerns are the reason the more sensitive PII fields (Birth year and Photo) were made "Optional". Also, TMS only collects the information necessary for the performance of its duties.

#### 5. Use of information

(a) **The intended use(s) for the information is/are:** The data is used to link the lender contact information to the loaned or purchased artwork. The loaned artwork is returned to the lender at the end of the exhibition; thus the need for address, phone, and email information. The lender's PII is retained in TMS as this tracks all works of art and its constituents. TMS serves as a reference for past loans and purchases. The birth year and headshot of the Lender is exported to the website along with the information of the artwork, i.e. (title, dimension, medium). The lender can be a museum, gallery or collector along with the artist. We collect contact information on the lender along with the artwork which they loaned.

(b) **Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?** Yes.

(c) **Does the system analyze the information stored in it?** Yes  No

If yes:

(1) **What types of methods are used to analyze the information?** TMS can run reports on the number of loans/exhibitions and locations the lender has been involved in.

(2) **Does the analysis result in new information?** No

(3) **Will the new information be placed in the individual's record?** Yes  No

(4) **With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?** Yes  No

## 6. Sharing of Information

(a) **With whom will the information be shared internally and/or externally?** Please identify the recipients of the information. No PII is shared with other systems or offices, inside or outside the Department.

(b) **What information will be shared?** No PII is shared with other systems.

(c) **The purpose for sharing the information is:** No PII is shared.

(d) **The information to be shared is transmitted or disclosed by what methods?** No PII is shared with other systems.

(e) **What safeguards are in place for each internal or external sharing arrangement?** Not applicable, no information is being shared

(f) **What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?** No privacy concerns exist, as PII is not shared.

## 7. Redress and Notification

**(a) What procedures allow individuals to gain access to their information?**

Individuals are not able to gain access to their information in TMS. No individuals outside of authorized Department Arts in Embassies staff users have access to the system.

**(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information? Yes X No \_\_\_\_\_**

**(c) By what means are individuals notified of the procedures to correct their information?**

They are notified directly via email or phone if it is found that information needs to be updated.

## 8. Security Controls

**(a) How is the information in the system secured?**

1. Access to the system requires an active DOS user account
2. That account must be matched to an active account created in the SQL database, which can only be created by an SQL Administrator and upon approval by the program office (AIE)
3. No one, other than the SQL Administrator has administrator access to the database itself

**(b) Describe the procedures established to limit access to only those individuals who have an “official” need to access the information in their work capacity.**

As stated above, only AIE staff (about 10 users) access the TMS system as their entire workday is built around this system.

**(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?**

1. AIE has an Audit trail which can track changes to the information.
2. Server monitoring is in place to monitor server access and escalation of privileges
3. Database administrators conduct reviews of database audit log files daily

**(d) Explain the privacy training provided to authorized users of the system.**

AIE staff is given instruction to which PII is optional information to obtain from lenders. Additionally, all users of the Department’s OpenNet system must take annual Cybersecurity Awareness Training.

**(e) Are any security controls such as encryption, strong authentication procedures, or other controls in place to make the information unusable to unauthorized users? Yes X No \_\_\_\_\_**

**If yes, please explain.** Strong authentication procedures require all DoS employees to use Department-issued PIV cards for access to OpenNet, and access to OpenNet is required before you can gain access to TMS.

**(f) How were the security measures above influenced by the type of information collected?**

The collection of PII makes the TMS system a Moderate impact system if confidentiality, integrity, or availability was compromised. As such, Moderate level security controls have been applied to the protection of the data.

**9. Data Access**

**(a) Who has access to data in the system?** All AIE employees (10-15)

**(b) Access to data in the system is determined by:** Senior Curator

**(c) Are procedures, controls or responsibilities regarding access to data in the system documented?** Yes X\_\_\_ No \_\_\_

**(d) Will all users have access to all data in the system or will user access be restricted? Please explain.**

User access is restricted based on need, with some users only having read rights.

**(e) What controls are in place to prevent the misuse (i.e. unauthorized browsing) of data by users having access to the data?**

1. Restrictive access by roles
2. Annual Privacy training
3. Enforcement of the TMS Rules of Behavior