Institute of Museum and Library Services

Privacy Impact Assessment

for

IMLS.gov (Drupal CMS)

9/27/2023

Institute of Museum and Library Services Privacy Impact Assessment

IMLS.gov (Drupal CMS)

Under the E-Government Act of 2002, the Institute of Museum and Library Services ("IMLS") must perform a Privacy Impact Assessment (PIA) (i) before initiating a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government); or (ii) before developing or procuring information technology systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public.

Section 1. Description of the system/project

Please provide a description of the information system or project in plain language. If it would enhance the public's understanding of the system or project, please provide a system diagram.

IMLS.gov is a major application developed using Drupal CMS and is located in AWS GovCloud. The IMLS public website (www.imls.gov) is one of the primary channels through which the agency informs the public, library/museum communities, Congress, and other organizations about its mission, goals, strategy, and the impact of agency grants on the wide range of communities across United States.

The sources of the data are: data feed ingested into Data Warehouse from the IMLS grants management system (eGMS), State Program Report (SPR), State Library Administrative Agencies (SLAAs), and the Public Libraries Survey (PLS); analytical data based on the aggregation logic residing in the Data Warehouse; static content provided by IMLS Program Offices; feedback and FOIA requests from the public; discussion forums, and applications from prospective library and museum reviewers.

In your description, please be sure to address the following:

a. *The purpose that the system/project is designed to serve.*
b. *Whether it is a general support system, major application, or other type of system/project.*
c. *System/project location (e.g., within Microsoft Azure, Qualtrics, Drupal, etc.).*
d. *How information in the system/project is retrieved by the user.*
e. *Any information sharing.*

Section 2. Information Collected

2.1 Indicate below what personally identifiable information (PII) is collected, maintained, and/or disseminated by your system/project (check all that apply).

Identifying numbers (IN)					
a. Social security number (full or truncated form)*		b. Driver's License		c. Financial Account	
d. Taxpayer ID		e. Passport		f. Financial Transaction	
g. Employer/Employee ID		h. Credit Card		i. U.S. Citizenship and Immigration Services	
j. File/Grant ID	x				
k. Other identifying numbers:					
* Explanation for the need to collect, maintain, or disseminate the Social Security Number:					

General Personal Data (GPD)					
a. Name	x	b. Maiden Name		c. Email Address	x
d. Date of Birth		e. Home Address		f. Age	
g. Gender		h. Personal Telephone Number		i. Education	x
j. Marital Status		k. Race/Ethnicity			
l. Other general personal data:					

Work-related data					
a. Occupation		b. Job Title	x	c. Work Email Address	x
d. Work Address	x	e. Work Telephone Number	x	f. Salary	
g. Employment History		h. Procurement/Contracting Records		i. Employment Performance Rating	
j. Other work-related data:					

System Administration/Audit Data					
a. IP Address	x	b. User ID/Username		c. Date/Time of Access	
d. Queries Run		e. ID of Files Accessed		f. Personal Identity Verification (PIV) Card	
Other system administration/audit data:					

2.2 Indicate sources of the information in the system/project and explain how the information is received.

Source of Information	**Explanation**
Directly From the Individual About Whom the Information Pertains:	Data feed ingested into Data Warehouse from IMLS Electronic Grants Management System (eGMS), State Program Report (SPR), SLAAs, discussion, forums, and PLS. Applications from potential library and museum reviewers.
Government Sources:	IMLS Program offices.
Non-Government Sources:	
Other:	

2.3 Whose data is collected, disseminated, disclosed, used, or maintained by the system / project? Please also provide an estimate of the number of individuals and minors within each category whose PII is contained within the system/project.

Members of the public	Approximately 800 members of the museum field who voluntarily apply to serve as peer reviewers but are not selected. No minors.
IMLS employees/contractors	Staff name, email, and work phone numbers are published on the website.
Other (explain)	Approximately 325 members of the museum field who voluntarily apply to serve as peer reviewers and are selected to serve. No minors.

2.4 Provide the legal authority that permits the collection, dissemination, disclosure, use, and/or maintenance of the PII mentioned in Section 2.1. (e.g., Section 9141 of the Museum and Library Services Act of 2018 (20 U.S.C. Ch. 72), OMB Circular A-130, etc.)

The information in this system is collected, maintained, and disseminated pursuant to the Museum and Library Services Act of 2018 (20 U.S.C. Ch. 72).

2.5 Describe how the accuracy of the information in the system/project is ensured.

Website relies on program office staff to ensure content is accurate by constantly monitoring and updating the information as required. Other information collected from the general public and reviewers is self-reported.

2.6 Is the information covered by the Paperwork Reduction Act?

Yes? Please include the OMB control number and the agency number for the collection.	No?
OMB Control #: 3137-0099, Expiration Date: 6/30/2024	

2.7 What is the records retention schedule approved by the National Archives and Records Administration (NARA) for the records contained in this system/project?

File plans and records retention schedules are currently being worked on.

2.8 Is the PII within this system/project disposed of according to the records disposition schedule?

File plans and records retention schedules are currently being worked on.

Section 3. Purpose and Use

3.1 Indicate why the PII in the system/project is being collected, maintained, or disseminated (e.g., for administrative purposes, to improve our services, etc.).

For internal and administrative purposes and to inform the public about the agency's employees and partners in the library and museum field.

3.2 Indicate whether the system collects only the minimum amount required to achieve the purpose stated in response to Question 3.1.

Yes, the agency ensures that the system is collecting and maintaining the minimum amount of information required.

3.3 Indicate how you intend to use the information to achieve the purpose stated in Question 3.1 (e.g., to verify existing data, to verify identification, to administer grant aid, etc.).

To contact individuals placing FOIA requests, to respond to individuals seeking to contact us, and for potential reviewers to apply to serve on panels for the agency.

3.4 Does the system use or interconnect with any of the following technologies? (Check all that apply.)

Social Media	x
Web-based Application (e.g., SharePoint)	x
Data Aggregation/Analytics	x
Artificial Intelligence/Machine Learning	
Persistent Tracking Technology	x
Cloud Computing	x
Personal Identity Verification (PIV) Cards	
None of these	

Section 4. Information Security and Safeguards

4.1 Does this system/project connect, obtain data from, or share PII with any other IMLS systems or projects?

Yes? Explain.	Data feed ingested into Data Warehouse from IMLS grants management system (eGMS), State Program Report (SPR), SLAAs, and PLS.
No, this system/project does not connect with, obtain data from, or share PII with any other IMLS system or project.	

4.2 Does this system/project connect, obtain data from, or share PII with any external (non-IMLS) systems or projects?

Yes? Explain. (Please also describe the type of PII shared, the purpose for sharing it, the name of the information sharing agreement, and how the PII will be shared.)		
No, this system/project does not connect with, obtain data from, or share PII with any external system or project.		x

4.3 Describe any de-identification methods used to manage privacy risks, if applicable.

n/a

4.4 Identify who will have access to the system/project and the PII.

Members of the public	
IMLS employees/ contractors	X (limited to specific employees)
Other (explain)	

4.5 Does the system/project maintain an audit or access log?

Yes? Explain. (Including what information is compiled in the log)	Yes, system admin logs and Google analytics.	
No, this system/project does not compile an audit or access log.		

4.6 What administrative, technical, and physical safeguards are in place to protect the PII in the system/project?

Access to the data collected requires administrative access with multi-factor authentication and the access is limited to very few IMLS employees. IMLS limits the users' rights to only what are strictly required to do their jobs (least-privileged access).

4.7 What are the privacy risks associated with the system/project and how are those risks mitigated (e.g., automated privacy controls, privacy training, etc.)? Please include a description of the technology used to protect PII in the system/project.

Privacy risk is low as the information collected is either public information, work-related data, or is not sensitive PII. PII such as name, email, phone number, etc. are safeguarded as described in 4.6.

4.8 Under NIST FIPS Publication 199, what is the security categorization of the system / project? Low, Moderate, or High?[1] (Please contact OCIO if you do not know.)

[1] Federal Information Processing Standards Publication 199 defines three levels of potential impact on organizations and/or individuals should there be a breach of security. The potential impact is defined as low if "[t]he loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals." Nat'l Inst. of Standards and Tech., *Fed. Info. Processing Standards Publ'n 199, Standards for Security Categorization of Federal Information and Information Systems* 2 (2004), https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf (emphasis omitted). The potential impact is defined as moderate if "[t]he loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations,

Low	x
Moderate	
High	

4.9 Please describe any monitoring, testing, or evaluation conducted on a regular basis to ensure the security controls continue to work as intended to safeguard the PII within the system/project.

IMLS.gov, as a major application, goes through comprehensive security assessment once every three years and is continuously monitored using vulnerability scans and EDR.

organizational assets, or individuals." *Id.* (emphasis omitted). The potential impact is high if "[t]he loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals." *Id.* at 3 (emphasis omitted).

Section 5. Notice and Consent

5.1 Indicate whether individuals will be notified that their PII is being collected, maintained, or disseminated. (Check the box or expand on the response that applies.)

Yes, notice is provided through a system of records notice (SORN) that was published in the Federal Register and is discussed in the next section.	X (eGMS)
Yes, notice is provided through a Privacy Act statement, privacy policy, PIA, or privacy notice. The Privacy Act statement, PIA, privacy policy, and/or the privacy notice can be found at (provide text of the notice if a link isn't available):	IMLS.gov privacy policy, available at https://www.imls.gov/privacyterms.
Yes, notice is provided by other means:	
No, notice is not provided. Please explain why:	

5.2 Please describe whether individuals are given the opportunity to consent to uses of their PII, decline to provide PII, or opt out of the system/project. Specify how below.

Consent	Yes, individuals have the opportunity to consent to uses of their PII:	x
	No, individuals do not have the opportunity to consent to uses of their PII.	
Decline	Yes, individuals have the opportunity to decline to provide their PII:	x
	No, individuals do not have the opportunity to decline to provide their PII.	
Opt out of	Yes, individuals have the opportunity to opt-out of the system/project:	x
	No, individuals do not have the opportunity to opt out of the system/project.	

5.3 Please describe what, if any, procedures exist to allow individuals the opportunity to review or request amendment or correction of the PII maintained about them in the system/project.

All PII collected/stored is self-reported; if a user would like to amend information collected about them by one of the program offices they can reach out and the agency will ensure that is carried out.

Section 6. Privacy Act

6.1 Is a "system of records" being created under the Privacy Act?

The Privacy Act of 1974 defines a "system of records" as "a group of any records . . . from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."[2]

Yes, a "system of records" is created by this system/project.	X (eGMS)
No, a "system of records" is not created by this system/project.	

[2] *See* Privacy Act of 1974, 5 U.S.C. § 552a(a)(5). https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf.

6.2 If you answered Yes to the previous question, please include a link to the system of records notice for this system/project. Or please indicate that we will need to create a new systems of records notice for this system/project.

https://www.imls.gov/sites/default/files/2019-21925.pdf

Section 7. Assessment Analysis

IMLS.gov has been determined to be of a low-risk impact to individuals. The system maintains primarily non-sensitive and work-related information. Furthermore, much of the information that the system collects is voluntarily provided by an individual which ensures that the collection is consensual, and individuals have opportunities to decline consent. The system security controls are continuously monitored, and the system underwent a comprehensive assessment in FY22.