Institute of Museum and Library Services

Privacy Impact Assessment
for
IMLS FOIA DATABASE

9/27/2023

Institute of Museum and Library Services Privacy Impact Assessment
IMLS FOIA Database

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.

The FOIA Database is a support system used to record, track, manage, and process requests in compliance with record access and disclosure requirements of the Freedom of Information Act, 5 U.S.C. § 552, and the Privacy Act of 1974, 5 U.S.C. § 552a. It is stored within the IMLS SharePoint Online, which is part of IMLS's general support system (GSS). Access is limited to those who have access to the OGC SharePoint, which includes OGC team members, interns, and selected IT team members. Information such as names and emails may be shared internally with IMLS staff in the process of responding fully to a request and/or tracking that request.

Requests are submitted either via the FOIA.gov website or the FOIA portal on IMLS's website. Both services ask for a name and email of the requester. Optionally, a requester can include a phone number and physical address in their submission.

A spreadsheet maintains all relevant information, including the FOIA tracking number, the requester's name and email address, and the information being requested, which often includes a grant number. The folders in the SharePoint Online contain further information, such as materials to be provided, including redacted versions of documents where appropriate. Taken together the spreadsheet and folders are the IMLS FOIA Database.

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	x	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: Occasional phone number, DUNS number					
* Explanation for the need to collect, maintain, or disseminate the Social Security Number: SSN is never disseminated or intentionally collected or maintained. Some requested grant applications mistakenly include an SSN which is redacted before being provided to the requester.					

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

Work-related data					
a. Occupation	x	b. Job Title	x	c. Work Email Address	x
d. Work Address	x	e. Work Telephone Number	x	f. Salary* *Salary not paid by IMLS grant funds is redacted*	x
g. Employment History		h. Procurement/Contracting Records	x	i. Employment Performance Rating	
j. Other work-related data:					

System Administration/Audit Data					
a. IP Address		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:	Requesters provide their own information including name, email address, and potentially phone number and mailing address.
Government Sources:	Applications are pulled from eGMS; which are pulled automatically from submissions to Grants.gov. Office of the Chief Financial Officer or Office of the Chief Information Officer occasionally provide copies of their records to fulfill a request.
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	Could range from 50-500 people, depending on number of requests received in a year and the nature of those requests. There is no data on minors collected, disseminated, disclosed, used, or maintained.
IMLS employees/ contractors	Could range from 50-500 people, depending on number of requests received in a year and the nature of those requests
Other (explain)	

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 USC Ch. 72), OMB Circular A-130, etc.)

The Freedom of Information Act, 5 U.S.C. § 552, and the Privacy Act of 1974, 5 U.S.C. § 552a. General Records Schedule (GRS) 4.2, item 020

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

Most information is user submitted, either via application or via request portal. For this information, the accuracy cannot be ensured. For documents that we provide, including grant IDs, care is taken to ensure that the correct response and relevant information/attachments are being sent to the correct requestor. For documents generated by IMLS offices, such as OCIO and OCFO, these documents are reviewed for any potentially inaccurate information.

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.	N/A
	X

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?

GRS 4.2 Item 020, Access and Disclosure Request Files. Destroy 6 years after final agency action or 3 years after final adjudication by the courts, whichever is later, but longer retention is authorized if required for business use.

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

Yes

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 administrative purposes and to fulfill agency responsibilities under the FOIA. Requester information such as name and email is never disseminated outside of IMLS.

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

Yes. As noted, occasionally people will provide far more than the minimum; those documents are redacted and/or sanitized appropriately before dissemination.

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

The information that is collected is used to respond to FOIA inquiries.

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

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

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.	eGMS and potentially other IMLS systems as is necessary to respond to the FOIA request.
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, or share PII with any external system or project.		X

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

PII such as personal emails, home addresses, personal phone numbers, and salaries not paid by government funds are redacted before a grant application is sent to a requester.

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

Members of the public	
IMLS employees/ contractors	OGC team members
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, versioning and access logs are available.	
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?

Redactions are used; no un-redacted documents or responses that contain PII are retained. Limited access control to OGC office only.

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.

There are minimal privacy risks. Direct access is limited to OGC team members, though selected information (name, email address, and information requested) may be shared with other offices to fulfill the request. OGC members with access have had privacy training.

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

Low	FOIA tracking database is Low Risk. However, it is part of the IMLS GSS which is FIPS199 Moderate.
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.

Please refer to IMLS GSS monitoring, testing and evaluation.

availability could be expected to have a serious adverse effect on organizational operations, 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.	
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):	
Yes, notice is provided by other means:	Grant applicants are informed that applications may be made publicly available through the NOFOs and in the grant's terms and conditions.
No, notice is not provided. Please explain why:	FOIA requesters are not directly notified that their names and email addresses will be retained for any period of time. This is consistent with other government sources and access points, including FOIA.gov, a DOJ-backed website.

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:		
	No, individuals do not have the opportunity to decline to provide their PII.		X
Opt out of	Yes, individuals have the opportunity to opt		

	out of the system/project:	
	No, individuals do not have the opportunity to opt out of the system / project.	X

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.

There are no procedures for correcting this information.

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

[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.

Section 7. **Assessment Analysis**

The FOIA Database contains information that is of low sensitivity to individuals. The database maintains only the minimal PII required to respond to the FOIA request. All files that are shared in responding to the FOIA request redact PII and any other personal information that is not relevant to the FOIA request. The FOIA Database is located on the IMLS SharePoint Online which is part of GSS. IMLS GSS has appropriate controls for access to information which will be inherited by FOIA.