Template 8.2023

Institute of Museum and Library Services

Privacy Impact Assessment

for

Reviewer History Database

9/27/2023

Institute of Museum and Library Services Privacy Impact Assessment

Reviewer History 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 purpose of this Access database is to allow Office of Museum Services (OMS) staff to track and assess past service of museum grant reviewers. A new set of reviewers is added to the database annually. The database is part of the IMLS general support system (GSS) due to its location within Microsoft Azure. The database is populated with data from eGMS and OMS staff. It is accessed only by OMS staff and is not available to the public.

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					
k. Other identifying numbers: eGMS Review Group number, eGMS ID					
* 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	
d. Date of Birth		e. Home Address		f. Age	
g. Gender		h. Personal Telephone Number		i. Education	
j. Marital Status		k. Race/Ethnicity			
l. Other general personal data:					

Work-related data					
a. Occupation		b. Job Title		c. Work Email Address	
d. Work Address		e. Work Telephone Number		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		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:	
Government Sources:	Name and review group numbers are exported from eGMS.
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	
IMLS employees/ contractors	
Other (explain)	Approximately 325 members of the museum field annually 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.).

20 U.S. Code § 9105 (c)–(d) (Museum and Library Services Act of 2018)

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

OMS exports the data annually from eGMS. The reviewers input information about themselves.

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?
	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?

This database is not on the OMS file plan. There are no records in the database.

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

This database is not on the OMS file plan. There are no records in the database.

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.).

The PII is collected for internal, administrative purposes.

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

The minimum amount of information is collected to achieve the goals of the database.

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.).

OMS uses the database when choosing reviewers for the current year.

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.	Data regarding reviewer history is imported from eGMS.
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	Only OMS staff
Other (explain)	

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

Yes? Explain. (Including what information is compiled in the log)	
No, this system/project does not compile an audit or access log.	**X**

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

The database is stored on the IMLS system, which requires password/PIV card to 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.

There are very few risks associated with the Reviewer History database. These risks are mitigated through privacy training for employees and controls on who can access the database.

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.)

Low	The Reviewer History Database is low risk. However, the system it is located within, IMLS's GSS, is FIPS199 Moderate.
Moderate	
High	

[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, 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).

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 the IMLS GSS PIA for information on how the system is monitored, tested, and evaluated.

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):	NEH's privacy policy on the eGMS Reach website and through the eGMS SORN from IMLS, these are available at https://www.neh.gov/privacy and https://imls.gov/about/policy/policy-notices/privacy-terms-use/privacy-program/imls-systems-records, respectively.
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:	Reviewers affirmatively choose to apply and serve as reviewers.	
	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.

Only name and review group are stored in the system. It is exported from eGMS. Individuals input their name each year and the information are sourced directly from the individual which ensures that the information is accurate.

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

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 system of records notice for this system/project.

The minute information contained in this database is covered by the "IMLS-1 IMLS Reviewers—Automated Systems" SORN, which can be found at the following link https://imls.gov/about/policy/policy-notices/privacy-terms-use/privacy-program/imls-systems-records.

[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.

Section 7. Assessment Analysis

The Reviewer History Database contains information that is of low sensitivity to individuals. This information creates minimal privacy risk given the minimal PII it contains and the temporary nature of the Access Database. The Access Database is located on the IMLS Azure server which is part of GSS and is monitored continuously. The IMLS GSS has appropriate controls for access to information which are inherited by the Reviewer History Database.