Template 8.2023

Institute of Museum and Library Services

Privacy Impact Assessment

for

IMLS Electronic Grants Management System
(eGMS and eGMS Reach)

9/27/2023

Institute of Museum and Library Services Privacy Impact Assessment

IMLS Electronic Grants Management System (eGMS)

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

IMLS's Electronic Grants Management System (eGMS) is a major web application that centralizes key aspects of the grant life cycle, including accepting applications submitted through Grants.gov; checking them for institutional eligibility and completeness; managing peer review; making awards; accepting and processing performance reports, financial reports, and payment requests; and generating closeout documentation. It is our officially sanctioned system for communicating with reviewers and awardees, and it complements our financial system, thereby facilitating a variety of quantitative and qualitative analyses and reports of our grant-making. A paired application, eGMS Reach, accommodates the grants management needs of our awardees (see below for details).

As a cloud system, eGMS is located in Microsoft Azure. It has an active authorization to operate from the hosting agency, the National Endowment for the Humanities, and its use and administration at IMLS are the responsibility of the Office of Grants Policy and Management (OGPM). Internal users are assigned to one or more of 13 user groups and have levels of access determined by need as authorized by their supervisors and approved by OGPM staff. A series of detailed job aids available on the agency's intranet provide how-to guidance for all functions.

External users with active awards have access to their applications and reports, IMLS decision notifications, messaging, and the capability of submitting reports and payment requests through the paired externally facing application, eGMS Reach. Users log in to eGMS Reach through Login.gov, which provides an extra element of secure private access. Job aids for their work are available on the agency's website. Access is terminated when an individual is no longer associated with a particular award. Peer reviewers have access to the applications assigned to them and to forms through which they record their scores and comments through eGMS Reach. IMLS staff terminate reviewer access when the review effort concludes.

eGMS collects personal information, such as mailing addresses, telephone numbers, email addresses, and resumes, through system-to-system ingestion of applications submitted to Grants.gov and directly from applicants, awardees, and peer reviewers through eGMS Reach. Staff access to and ability to modify this information is controlled internally through restrictions associated with user groups.

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.

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: Institutional TIN/EIN.					
* 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	X	b. Job Title	X	c. Work Email Address	X
d. Work Address	X	e. Work Telephone Number	X	f. Salary	X
g. Employment History	X	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	X	c. Date/Time of Access	X
d. Queries Run	X	e. ID of Files Accessed	X	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:	Names of individuals, work email addresses, work mail addresses, work telephone numbers, institutional affiliations, education information, areas of expertise, descriptions of work experience, and resumes are collected through eGMS Reach from award participants who are new to a project and from peer reviewers. The data necessary to create a People record is entered manually for integration into the eGMS system.
Government Sources:	IMLS routinely extracts information from SAM.gov through APIs in order to review institutions' names, addresses, registrations, owners, proceedings, EINs, past performance on grants from other agencies, and POCs (names, job titles, email addresses, telephone numbers) so that we may conduct required checks before making awards. IMLS may consult relevant IRS databases to confirm non-profit status of applicants.
Non-Government Sources:	IMLS staff frequently consult applicant websites to verify information on applications and to view grant products as part of their review of performance reports.
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	Participants in active awards (e.g., Project Directors, Grant Administrators, Authorizing Officials, Financial Staff): There is a minimum of two individuals associated with each active award and there can be as many as five or six. All participants are sanctioned by the Authorizing Official. As of this writing, there are 2200 open awards. Peer reviewers: Est. 350-450 per year. There is no data on minors collected, disseminated, disclosed, used, or maintained.
IMLS employees/ contractors	OLS, OMS, OGPM staff
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 U.S.C. Ch. 72), OMB Circular A-130).

The Museum and Library Services Act (20 U.S.C. § 9141); 20 U.S.C. § 80u(f) (National Museum of the American Latino, Educational and liaison programs); 20 U.S.C. §§ 80r–80r-9 (National Museum of African American History and Culture), in particular 20 U.S.C. § 80r-5 (Educational and liaison programs).

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

OGPM sends an electronic “tip for success” each month to individuals designated in eGMS as participants in open awards. If a message is undeliverable or if an auto-reply indicates that a participant has left the project or the organization, we follow through to secure updated/corrected information and make the appropriate changes in eGMS. Institutional information is checked against existing eGMS records and against SAM.gov at the beginning stage of processing grant applications and each time an awardee requests payment. Any discrepancies or apparent errors are investigated, and we make the appropriate changes in eGMS.

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?
Each of our grant programs is associated with an OMB control number. In some cases two grant programs share one control number. The numbers are: 3137-0091; -0093; -0094; -0095; -0097; -0102; -0103; -0107; -0110; -0111; -0123; -0134. Our forms are also associated with OMB control numbers: 3137-0089; -0092; -0098; -0099; -0100; -0124; -0126.	

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?

Records are permanent and are not destroyed. Files may be destroyed ten years after final action is taken on the file, 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?

We began using eGMS October 1, 2019, and we have not yet operationalized the destruction of records ten years after the final action is taken on a file. It is important to note that eGMS never automatically deletes information. Only IMLS staff with appropriate permissions can manually delete information.

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).

PII is collected and maintained for administrative purposes. We must be able to communicate with our awardees and peer reviewers and use the eGMS system to do so. Information is also used in the evaluation of applications for federal assistance and in the processing of disbursements of grant funds.

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

We collect only the minimum amount required to maintain communication, and it is typically work-based information (rather than home-based) that we collect and maintain.

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).

We use this information to evaluate applications for federal assistance, manage the peer review process, manage active grants, maintain communication with awardees, and accept payment requests.

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)	X
Data Aggregation/Analytics	X
Artificial Intelligence/Machine Learning	X
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, or share PII with any other IMLS systems or projects?

Yes? Explain.	IMLS may publicly disclose information pertaining to funded projects on its website, in announcements to Congress, or via press releases.
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.)	Yes, Sam.gov and Grants.gov. SAM.gov: eGMS displays information about an applicant/awardee organization's SAM status, expiration date, whether or not they have delinquent federal debt, and whether there are any known exclusions. NEH manages that connection using the API that SAM provides. All this information is available to the public through SAM.gov. Grants.gov: eGMS pulls application files (which include mailing addresses, telephone numbers, email addresses, and resumes as provided by the applicant) from Grants.gov through a system-to-system interface as described in Section 1.
No, this system / project does not connect with, obtain, or share PII with any external system or project.	

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	Participants in active awards have access to information about their own awards. Peer reviewers have limited access to review applications assigned to them.
IMLS employees/contractors	Office of Library Services, Office of Museum Services, Office of Grants Policy and Management, Office of the Chief Financial

	Officer, and Office of the General counsel staff, and in limited situations contractors, have access at varied levels structured according to permissions associated with specific user group(s).
Other (explain)	

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

Yes? Explain. (Including what information is compiled in the log)	Activity logs are automatically created for every action taken by a user in eGMS. These logs identify what actions were run by which users and when. These logs are saved permanently, and reports are run and examined routinely in order to detect and identify potential misuse.
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 by IMLS staff is restricted via controls associated with specific user groups, which are carefully monitored. Permissions of staff whose job responsibilities change or who leave the agency are modified (or eliminated) immediately. Award participants have access only to the information associated with their awards. Peer reviewers have access only to those applications assigned to them, and this is only for the duration of the relevant review cycle.

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)? Please include a description of the technology used to protect PII in the system/project.

The risk of inadvertent disclosure of awardee or peer reviewer information is mitigated by restricting access to authorized users in keeping with permissions associated with specific user groups.

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	
Moderate	**X**
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 Technology 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.

IMLS has a System Security Plan (SSP) for eGMS that details regular monitoring, testing, and evaluation of eGMS and eGMS reach. These protocols work to ensure that the PII within the system is being safeguarded.

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**
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):	Also, the NEH Privacy Policy and SORN are posted on eGMS Reach's website. They are available at https://www.neh.gov/privacy and https://www.neh.gov/sites/default/files/inline-files/neh_systems_of_records_notice.pdf.
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:	All disclosures of PII are voluntary as those providing information are freely applying for financial assistance or are freely seeking engagement as an IMLS peer reviewer.	
	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:	See above.	
	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:	See above.	
	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.

If IMLS staff identify any issues while reviewing applications for completeness and eligibility and/or while comparing information provided with existing information in eGMS for an applicant institution or a potential peer reviewer, they may notify the applicant or potential reviewer and provide an opportunity to correct or resubmit information.

Both applicants and reviewers can access information they have submitted through eGMS. Once an award is closed out, an awardee can access but can no longer make changes to the information they submitted. If someone identifies misinformation, they can contact IMLS staff to request a change.

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 systems of records notice for this system/project.

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

Section 7. Assessment Analysis

eGMS is a cloud-based web platform that IMLS shares with NEH, who hosts and manages the platform. NEH is primarily responsible for the information security of the system and ensuring compliance with the data and information security standards. However, IMLS believes that the access and security protocols are comprehensive and suitable for the level of sensitivity of the PII maintained in the system. IMLS continues to monitor the access our employees and grantees have to the system in addition to the eGMS FISMA Package developed by NEH.

[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.