Institute of Museum and Library Services

Privacy Impact Assessment

for

State Program Report (SPR)

9/27/2023

Institute of Museum and Library Services Privacy Impact Assessment

State Program Report (SPR)

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 State Program Report (SPR) is a reporting tool used by the 50 states, the District of Columbia, the U.S. territories, and the freely associate states for the IMLS Grants to States program. It provides states the ability to file annual financial and performance reports 120 days after the end of each period of performance, as well as interim federal financial reports within 90 days after the first year of performance, as required by law. The Financial Status Report provides detailed information on the expenditure of funds allotted to the state library administrative agency. It provides evidence that the state is meeting its matching and maintenance of effort requirements. The certification form verifies that the appropriate state official has approved all parts of the State Program Report for submission to IMLS. The narrative and quantitative Project information describes how funds were used, including budget detail that is not publicly available. The system is a major application, hosted in AWS GovCloud. State and IMLS users input and retrieve information in the system through the password-protected interface at https://imls-spr.imls.gov/Login. Within the system, they can download Excel data at the project and activity level for their state. Once projects are accepted, the general public can access them at https://imls-spr.imls.gov/Public/Projects, except for budget details and uploaded Additional Materials.

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	
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	**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	**X**	c. Date/Time of Access	**X**
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:	Project Directors submit reporting data to the states administering IMLS funds, who input it into the SPR system. This includes basic contact info.
Government Sources:	
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	Project directors responsible for the IMLS-funded projects. Estimated 500 individuals/year. There is no data collected, disseminated, disclosed, used, or maintained about minors.
IMLS employees/contractors	Estimated 10 individuals/year.
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, etc.).

2 C.F.R § 200.332 Requirements for pass-through entities 2 C.F.R. § 200.329(c)(1) Final Performance Reports 2 C.F.R. §§ 200.328, 200.329(c)(1) Annual (Interim) Reports Section 9134(b)(8) of 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.

Authorized Certifying Officials (ACOs) for each state sign annual SPR submissions, testifying to their completeness and accuracy, and they are then reviewed by IMLS Program Officers before reports are officially “accepted” by IMLS.

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?
Yes: OMB Control # 3137-0071, Expiration Date: 09/30/2025	

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?

Temporary. Destroy 10 years after the final report close-out for the last year in a Grants to States five-year cycle, but longer retention is authorized if required for business use (suggested IMLS disposition is no longer than 15 years).

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.).

In addition to administrative purposes, the outcomes of these significant federal investments are of interest to the field at large. When IMLS wants to showcase or follow-up on specific federally funded projects for more information, basic contact information is needed. The Public View of the SPR is meant to provide transparency and share best practices from the federal library investment, and non-IMLS staff may also want to follow up with project directors as well.

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 system collects the minimum amount of information to achieve the above purposes.

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.).

We intend to use the information to identify and occasionally contact the Project Directors of the institutions that utilize IMLS funds.

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	
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.	Yes, the contact info for 3-8 individuals from each state are collected in the State Info section of the SPR and manually entered in eGMS, in the required fields for each grant: Authorized Certifying Official, Project Director, Grant Administrator, Finance Contact, etc. The SPR preceded eGMS, and this transfer of info was designed to prevent duplication of information requests.
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.	No.

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	X (to the public facing SPR portal)
IMLS employees/ contractors	X
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. A User Management module is maintained for individuals with direct access to the system. We also maintain a server access log with usernames and time of access.
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?

States inputting data are instructed to provide only work contact info, much of which is already publicly accessible on institution websites. There are also regular access controls and multi-factor authentication so that people can only access the system on an as-needed basis.

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.

Almost all the PII data in the system is already publicly available because it is work-related contact information. Therefore, the privacy risks are low. IMLS relies on states to input the correct information and provides technical guidance on its website about the SPR fields, as well as annual training. However, IMLS program officers also review annual data and request changes before "accepting" projects, which renders them publicly accessible. The SPR technology access controls related to project status (e.g. draft, complete, certified) also keep PII from being released publicly prior to approval

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	**X**
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.

IMLS monitors the SPR system at least monthly, and often daily, as part of its regular monitoring and compliance activity for the grant program. There is a weekly standing meeting between Grants to States, OCIO staff, and IMLS contractors/developers to discuss and enhance the system. Additionally, the SPR system goes through continuous monitoring and a comprehensive security assessment once every three years.

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 systems and 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 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 https://imls-spr.imls.gov/Login (password-protected). "Welcome to the online reporting system for IMLS' State Grant Program. Before entering your data and descriptions, please take a moment to review this information about security and privacy. After reading the information, click the "I Accept" button to demonstrate that you understand and agree to the conditions below and are ready to enter the system. **Security and Accuracy of Information:** You are entering an Official United State Government System, which may be used only for authorized purposes. The Government may monitor and audit the usage of this system, and all persons are hereby notified that the use of this system constitutes consent to such monitoring and auditing. Unauthorized attempts to upload information and /or change information on this web site are strictly prohibited and are subject to prosecution under the Computer Fraud and Abuse Act of 1986 and Title 18 U.S.C. Sec. 1001 and 1030. Federal law provides criminal penalties of up to $10,000 or imprisonment of up to five years, or both for knowingly providing false information to an agency of the United States Government. 18 U.S.C. Section 1001. **Privacy:** Except as otherwise indicated, the information you submit through the online reporting system may be made publicly available through a public IMLS website. Information submitted to IMLS through the online reporting system may also be subject to disclosure as required by law under the Freedom of Information Act or other statutory provisions. For more information about privacy, please see our Privacy Policy."
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:	Yes. Consent is implied by responding to the federal collection of information.	
	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:	Yes. If an individual Project Director opted to not provide their PII, the state could include a state-level contact instead.	
	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:	Yes. The requirements for the system are at the project level, not the individual level.	
	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.

An individual can contact their state at the point of data entry/reporting to express any concerns, and the state can make adjustments to PII. If an individual's PII ends up in the system and they want it corrected/omitted, they can contact their state or IMLS (note that this has never happened to date).

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.	No, because records are not organized or retrieved by individual (but by state and 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.

n/a

[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 State Program Report (SPR) contains information that is low sensitivity to individuals. The data that is collected by the SPR is primarily work-related data as opposed to general personal data. IMLS has established appropriate privacy and security controls for access to the information based on the above-stated level of sensitivity. In the future, IMLS will need to do further analysis to implement Multi-Factor Authentication for logging into the non-public-facing SPR webpage.