Institute of Museum and Library Services

Privacy Impact Assessment

for

The IMLS General Support System

9/27/2023

Institute of Museum and Library Services Privacy Impact Assessment

for

The IMLS General Support System

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.

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.

IMLS creates, collects, uses, stores, maintains, disseminates, discloses and disposes of PII in support of its mission, which is to advance, support, and empower America's museums, libraries, and related organizations through grantmaking, research, and policy development.

The IMLS General Support System (GSS) provides connectivity, security, storage, communications, Internet access, and data access. The IMLS GSS is a collection of hardware, software, applications, databases, and communication systems hosted on-premises and Azure cloud systems using IaaS that form a networked infrastructure to support the IMLS's mission, daily operations, and data processing needs. The infrastructure includes OneDrive and SharePoint for data storage, Microsoft Exchange Online, Teams and SharePoint Online as a communication and collaboration platform, network services, access to Financial and HR systems, and secure VPN access to IMLS resources.

IMLS has interagency agreements with the Interior Business Center to manage payroll records and with the Enterprise Services Center to manage accounting records and transactions. Access to these external systems is through secure VPN connections.

IMLS GSS is in Microsoft Azure and the LAN Room.

Purpose type:

- Business Intelligence Services
- Collaboration Tools (SharePoint)
- Cybersecurity Monitoring
- Cybersecurity tools/solutions
- Data Repository
- Email services and/or internet access
- General Support System (GSS) [WAN/Mainframe/Gateway]
- General System and Infrastructure Support
- Local Area Network (LAN)
- Physical Access Control Systems (PACS)
- Procurement systems
- Trusted Internet Connection (TIC)

Section 2. <u>Information Collected</u>

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)*	**X**	b. Driver's License		c. Financial Account	**X**
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:
* Explanation for the need to collect, maintain, or disseminate the Social Security Number: IMLS is collecting this information in conformance with the Privacy Act of 1974. The information collected is confidential and will be used to process payment data from IMLS to the financial institution and/or its agent. Providing this information is voluntary; however, failure to provide the requested information may affect processing and may delay or prevent the receipt of payments.

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	**X**	i. Education	
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	
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	**X**	e. ID of Files Accessed	**X**	f. Personal Identity Verification (PIV) Card	**X**
Other system administration/audit data:					

Source of Information	**Explanation**

Directly From the Individual About Whom the Information Pertains:	• Data is maintained for individuals working for or transacting business with IMLS. • For employees, the data is provided as part of the employment process. • Employee work-related data stored in SharePoint online. • Emails sent and received by employees.
Government Sources:	• Administrative access logs.
Non-Government Sources:	
Other:	

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

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	**X (around 480 peer and field reviewers) There is no data on minors collected, disseminated, disclosed, used, or maintained.**
IMLS employees/contractors	**All IMLS employees and contractors.**
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 (20 U.S.C. § 9141), OMB Circular A-130, etc.)

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

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

- Employees are expected to adhere to IMLS policies and procedures to ensure the accuracy of the information.
- Employees take Annual Security Training that provides tips to ensure the accuracy of information received and sent.

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?

Records schedules are in the process of being finalized.

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

Refer to 2.7.

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.).

PII is collected for 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.

Yes, the system collects the minimum amount of information required for administrative and security 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.).

PII is collected by the system to verify the identity of individuals and ensure the integrity of the agency's infrastructure.

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	X
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.	
No, this system/project does not connect with, obtain data from, or share PII with any other IMLS system or project.	**X**

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, nor 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** (Authorized IMLS employees only)
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 logs.
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?

The Agency limits users' access 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.

Risks:

- Intentional/unintentional unauthorized internal access to private data
- Hacking by external sources
- Phishing

Mitigation Strategy:

- Access to GSS system is protected by VPN, MFA, PIV, Firewall and Zscaler only for authorized users.
- Access to IMLS data is limited to users' access rights strictly required to do their jobs (least-privileged access).
- Email and DNS filtering by using Accelerated (E3A) and Protective DNS.
- CISA CDM Shared Services (Qualys, CrowdStrike)

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	

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.

- Access to GSS system is protected by VPN, MFA, PIV, Firewall and Zscaler only for authorized users.
- Access to IMLS data is limited to users' access rights strictly required to do their jobs (least-privileged access).
- Email and DNS filtering by using Accelerated (E3A) and Protective DNS.
- CISA CDM Shared Services (Qualys, CrowdStrike).

Notice and Consent

5.10 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	**X** (imls.gov privacy policy and PIA):
	https://www.imls.gov/privacyterms;
	https://www.imls.gov/privacy;

[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).

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):	https://www.imls.gov/about/policy/policy-notices/privacy-terms-use/privacy-program/privacy-impact-assessments
Yes, notice is provided by other means:	
No, notice is not provided. Please explain why:	

5.11 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:	
	No, individuals do not have the opportunity to opt out of the system/project.	**X**

5.12 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.

Any changes to user PII should be approved by IMLS Human Resources.

Section 5. 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.

You can find the IMLS GSS SORN on IMLS’s privacy program page found at imls.gov/privacy.

[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 6. Assessment Analysis

The agency has determined that the vulnerability of PII maintained in the IMLS Network is low. The number of individual records is low, and the IMLS has established appropriate controls for access to information based on its level of sensitivity. Given the nature of the information collected, maintained, and disseminated by this system, IMLS has implemented measures to protect and enhance the security posture of the agency network which includes securing access for remote users, personal and agency furnished devices, and cloud-based assets. The agency's OCIO has embarked on a journey to transition its network to IPV6 and to implement Zero Trust Architecture (ZTA), completed the implementation of zScaler cloud security platform solution, and enrolled in the DHS/CISA Continuous Diagnostics and Mitigation (CDM) program for Vulnerability, Configuration and Asset Management (Qulays), and Endpoint Detection and Response (CrowdStrike). IMLS's GSS has also gone through a comprehensive Security Assessment and Authorization, an independent evaluation, and has established a Vulnerability Disclosure Program (VDP) extended to multiple information systems. IMLS is currently working with the DHS (CISA) to implement further capabilities. Overall, IMLS's OCIO has developed policies and procedures that provide sufficient guidance and limitations for employees and other system users.