INSTITUTE of Museum and Library SERVICES

Privacy Impact Assessment

for

Public Libraries Survey

9/27/2023

Institute of Museum and Library Services Privacy Impact Assessment

Public Libraries Survey

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.

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 (for example, within Microsoft Azure, Qualtrics, Drupal, etc.).*
d. *How information in the system / project is retrieved by the user.*
e. *Any information sharing.*

The Public Libraries Survey (PLS) is a web-based data collection system that supports the annual census of public libraries in the 50 States, Washington DC, and the outlying territories. The PLS has two online interfaces that house personally identifiable information: the PLS Web Portal and the State Data Coordinator (SDC) Discussion Forum.

The PLS data collection operates through a standalone data collection tool (the PLS Web Portal) on AWS with a robust edit-check system to help with data quality. The Web Portal is currently hosted on AIR's AWS site, but OCIO is in the process of migrating the tool to IMLS's AWS site.

The PLS Web Portal collects contact information from State Data Coordinators (SDCs) and Chief Officers of State Library Administrative Agencies from each state who report or certify data, depending on their role.

The PLS is a federal survey that collects data from states on the libraries within their jurisdictions. Information on libraries includes identification, operating revenue and expenditures, number of full time equivalent (FTE) staff, public service hours, service outlets, collections, circulations, programs and attendance, and other services.

These data are the basis for a set of data files and other data products that IMLS releases each year on IMLS.gov, which include state benchmarking tables and an IMLS Library Search and Compare Tool. IMLS typically publishes a research report or brief, providing both current year and trend analyses.

To foster a community of practice amongst respondents, IMLS also hosts an SDC Discussion Forum built in Drupal Groups on IMLS.gov by IMLS IT contractors. The SDC user list is linked to the PLS Web Portal through an authentication process that allows “seamless” logon to IMLS.gov Groups through the PLS Web Portal. SDCs can also log in directly through IMLS.gov.

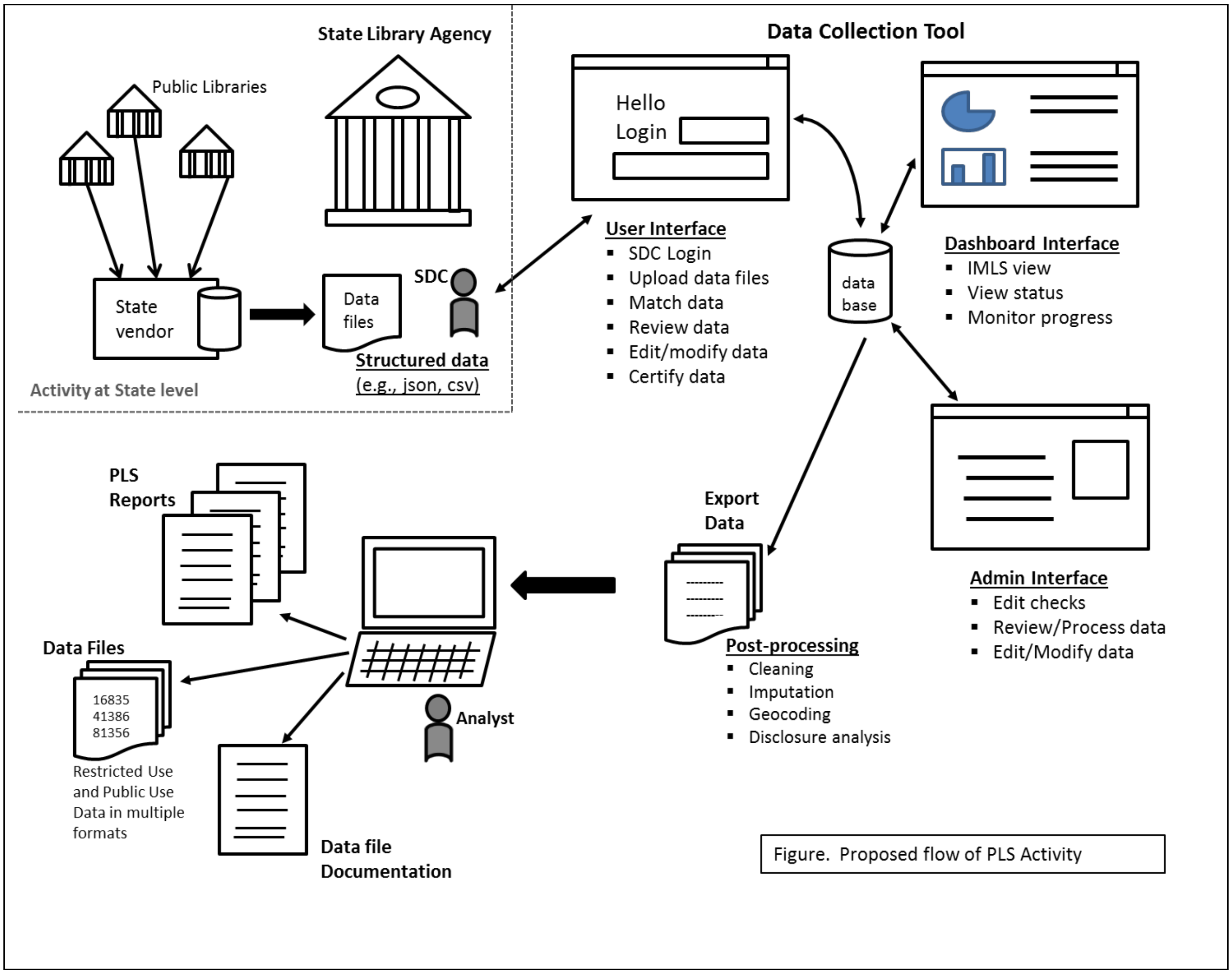

Figure. Proposed flow of PLS Activity

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/Employe e 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:					

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	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		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: **X** – AIR stores the stack trace in the web log for debugging purposes. This is only captured if an error is experienced by a user.					

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, work emails, work phone numbers and work addresses from State Data Coordinators and Chief Officers of State Library Administrative Agencies are volunteered by States and Chief Officers or other state representatives to support their official roles as respondents and certifiers of PLS data from their state or to allow for logging into to the SDC Discussion Forum on IMLS.gov.

Government Sources:	Names, work emails, work phone numbers and work addresses from State Data Coordinators and Chief Officers of State Library Administrative Agencies to support their roles as respondent and certifier of PLS data from their state.
Non-Government Sources:	Contractor names, work phone numbers, and work emails.
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	PLS Web Portal: Contact information is collected from 51 State Data Coordinators, employees of the State Library Administrative Agencies that each manage the State's collection of data from public libraries within their state. The Chief Officer certifies the survey data before final acceptance at IMLS. SDC Discussion Forum: Only the 51 SDCs, as respondents of the PLS, AIR contractors, and IMLS staff have access to the SDC Discussion Forum. There is no data on minors collected, disseminated, disclosed, used, or maintained.
IMLS employees/contractors	PLS Web Portal: Approximately 5–7 contractors (currently from AIR) working on behalf of IMLS annually update the PLS Web Portal to reflect changes to the survey instrument, provide training to SDCs, prepare collection materials, and manage the January–August data collection period. These contractors also prepare the data for public use and prepare research for dissemination efforts after the collection ends. IMLS employees review the PLS data for public dissemination. SDC Discussion Forum: AIR contractors and IMLS staff have access to the SDC Discussion Forum. IMLS also has IT contractors that support the Drupal Groups site on IMLS.gov.
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.).

IMLS collects these data under the mandate in the Museum and Library Services Act of 2018 (PL 115-410), as stated in section 9108. (20 U.S.C. Ch. 72)

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

Regarding PII of PLS respondents, IMLS sends out advance letters to SDCs and Chief Officers a couple of months before each data collection. Generally States keep IMLS informed of any changes to the contact information of the SDC, and IMLS keeps track of the Chief Officers through COSLA's website and the Grants to States' State Profiles page at https://www.imls.gov/grants/grants-state/state-profiles. Otherwise, the PLS Web Portal has a robust edit-check system to catch potential errors in library-level data submitted by the SDCs. SDCs are asked to review and correct or annotate critical edit checks. Chief Officers then certify the data after the SDC has submitted the files.

2.6 Is the information covered by the Paperwork Reduction Act?

OMB No. 3137-0074. Expires 11/30/2024.

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?

Currently unknown. ORE is working with OCIO on updating ORE's Records Management Plan.

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

Currently unknown. ORE is working with OCIO on updating ORE's Records Management Plan.

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.).

SDC and Chief Officer contact information is collected and maintained in the system since they are the respondents and certifiers, respectively, of their State's submission to IMLS' PLS Web Portal for the annual Public Libraries Survey collection.

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 only the minimum amount necessary, in most cases only the name, work email and work institution.

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 use the information to contact the SDCs and Chief Officers in October of each year in advance of the opening on the annual PLS collection the following January.

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	
Cloud Computing	X Cloud computing covers AWS and we do data aggregation/analytics in post-lock and post-processing.
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.	X. The PLS Web Portal and the SDC Discussion Forum are linked by SDC email and are connected to the IMLS website.

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.

States also report library-level salary and benefit expenditures for all libraries in their state. Historically, data suppression has been the primary disclosure limitation method employed for the PLS. This method provides sufficient protection against disclosure. The selected expenditures data of public libraries noted in the preceding list (i.e., Salaries & Wages Expenditures, Employee Benefits Expenditures, Total Staff Expenditures, and Other Operating Expenditures) will be set to -9 and the observation flagged as H_16 in the imputation flag variable on the public-use Public Library System Data File when their total FTE staff is less than or equal to 2.00. In states where only one or two libraries have suppressed data, these data points will be suppressed for one to two other libraries within the same state to ensure that all states that have suppressed data have a minimum of three suppressed records to prevent disclosure of the otherwise suppressed data.

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

Members of the public	State Data Coordinators and Chief Officers of State Library Administrative Agencies
IMLS employees/contractors	Marisa Pelczar, AIR contractors, IT staff and contractors
Other (explain)	

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

Yes? Explain. (Including what information is compiled in the log)	The PLS Web Portal provides system logging and monitoring to facilitate auditing and accountability. This includes selecting auditable events required to contain the following information at a minimum to establish what events occurred, the sources of the event, and the outcomes of the events: • Source User ID • Event timestamp (Date & Time) • Event Details • Type • Outcome (success/failure) • URL and URL Referrer • HTTP Method • Status Code • Form • Parameters • Event Message (stack trace) • Source/Target Host
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?

AIR has a comprehensive information security program that is documented in the AIR Information Security Policy. The AIR Information Security Program is designed to provide a framework to manage physical and cybersecurity risks while meeting federal, state, and industry information security requirements.

The server environment in use for the PLS Web Portal is hosted in the AWS FedRAMP-compliant cloud. Our infrastructure is supported by a team of highly trained information security staff, IT network security engineers, and system administrators that design, operate, manage, and monitor a reliable, secure, and compliant infrastructure and web hosting environment. The infrastructure staff have significant experience on both Azure and AWS FedRAMP-certified infrastructure. Systems that store project data are protected by a defense-in-depth network architecture. All protection systems are continuously tuned and monitored to address the latest cyber threats. All servers adhere to configuration baselines established by the Center for Internet Security (CIS). Role-based access control enables precisely focused access management for the cloud environment. Servers are configured with encryption at either file, volume, or disk level. AIR employs malware protection for all servers and endpoints. The AWS cloud infrastructure is configured with two-factor authentication.

AIR implements security logging on infrastructure servers and network devices that are forwarded to a central security information and event management (SIEM) system. There, our logs are indexed and correlated to facilitate incident response searches, log analysis, and to support after-the-fact investigations. Dedicated cybersecurity staff continually monitor the SIEM to properly identify and respond to commodity and advanced persistent threats. AIR IT and Infosec staff have significant experience in performing vulnerability remediation in accordance with internal and external remediation objectives and before threats can exploit them.

At the application layer, only authorized internal and external users have access to the PLS Web Portal and SDC Discussion Forums. Accounts are established based on the States' designation of individuals as SDCs for that cycle.

PLS project data is stored and analyzed on secure servers, both of which are also FedRAMP-compliant (one is cloud-based, the other solid-state). Until the data is processed/suppressed it does not leave the secure servers.

When individuals leave their SDC or CO roles, IMLS or contractors remove their accounts from the PLS Web Portal and SDC Discussion Forum.

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.

A privacy risk could entail human error related to database management. AIR addresses this risk through the application of several controls identified in the system security plan (access controls, configuration management, audit and accounting, identification and authorization, boundary controls, etc.).

An additional risk is account sharing. Though they are told not to, IMLS and AIR cannot control if a Chief Officer shares their Web Portal credentials with their SDC. AIR has email verification enabled when a Web Portal user attempts a password reset.

Also, as discussed above, salary and benefit information is collected as part of the data submission. AIR suppresses this data for any library that reports 2 or fewer staff.

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.

AIR and OCIO regularly update the System Security Plan for the PLS Web Portal, ensuring all security controls necessary for FISMA Low are completed. In 2022, the PLS Web Portal underwent a full scope assessment for a FISMA Low security categorization system.

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:	
No, notice is not provided. Please explain why:	X Notice is not provided by IMLS as the contact information is generally volunteered by the State Library Administrative Agency. There will be a privacy notice added to the PLS portal.

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:	
	No, individuals do not have the opportunity to consent to uses of their PII.	X
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.

SDCs are encouraged to reach out to IMLS or the contractor with changes to their work emails to ensure that IMLS can successfully communicate with the SDCs before and during the PLS data collection period.

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

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 PLS contains information that is of low sensitivity to individuals. The contractor who is hosting the PLS web portal and discussion forum has ensured that it is stored on a FedRAMP-compliant cloud, is continuously monitored, and is encrypted. The agency has created policies and procedures that ensure the safety

[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.

of the information maintained in this system. The agency will create a privacy notice for the PLS web portal this year.