Protecting Sensitive Data at IMLS

IMLS is committed to protecting your private, sensitive information and employs the following physical and technical safeguards when collecting museum program reviewer and panelist information:

1. *Email Security.* IMLS email is hosted on a cloud computing infrastructure which has been reviewed and approved as meeting the security requirements of the *Federal Risk and Authorization Management Program* (FedRAMP). FedRAMP is a government-wide standardized program for security assessment, authorization, and monitoring of cloud products and services. FedRAMP requirements are based on (and surpass) the *Security and Privacy Controls for Federal Information Systems and Organizations* developed by the National Institute of Standards and Technology. FedRAMP's additional security controls address the unique elements of cloud computing to ensure all federal data is secure in cloud environments.

2. *Secure File Transmission*. IMLS Secure File Upload uses Hypertext Transfer Protocol Secure (HTTPS), a transmission protocol that verifies the identity of a website or web service for a connecting client, and encrypts nearly all information sent between the website or service and the user. HTTPS is designed to prevent this information from being read or changed while in transit. HTTPS is a combination of HTTP and Transport Layer Security (TLS). TLS is a network protocol that establishes an encrypted connection to an authenticated peer over an untrusted network.

3. *Secure File Storage.* IMLS will only store secure files and any related passwords as long as necessary to complete the relevant transaction or process. A physical copy of personally identifiable information (PII) may be printed at IMLS for business use, after which the copy is secured in a locked location and destroyed after the business use ceases.

4. *Access Controls.* IMLS employs access controls to restrict access to sensitive information that is stored electronically. Access to IMLS files is restricted to authorized IMLS staff, and sensitive data is stored in folders that can only be accessed by a restricted set of authorized users. Files containing sensitive information are password-protected, providing an additional layer of security.

5. *Records Policies.* IMLS financial transaction records are subject to the agency's record retention policy and disposed of in accordance with the General Services Administration's General Records Schedule.