Institute of Museum and Library Services

Privacy Impact Assessment

for

GovDelivery by Granicus

Institute of Museum and Library Services Privacy Impact Assessment

GovDelivery by Granicus

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

1.1 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 agency employee.

e. Any information sharing.

Granicus is a cloud-based digital communications platform that helps government organizations manage citizen engagement. The Granicus GovDelivery platform is a web-based email marketing software as a service that primarily helps organizations create branded emails, websites, online stores and more in one online marketing platform. IMLS uses the GovDelivery platform to (1) maintain a subscribed user list for news releases, blogs, research announcements, and monthly newsletters; (2) distribute event invitations, and (3) connect with past, present, and potential grantees about panels, reviewer opportunities, and webinar information via email distribution lists.

Names and email addresses are stored on the platform. Subscribers are sorted into lists of their choosing. Professional contacts for invitations or targeted communications are uploaded from contacts in IMLS' electronic Grants Management System (eGMS) system and maintained in specifically labeled, limited use distribution lists.

Granicus does not sell or rent email addresses. Users are not permitted to upload or use purchased, traded, shared, or borrowed lists to their Granicus account. Similarly, IMLS does not sell or share its email lists.

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					
k. Other identifying numbers:					
* Explanation for the need to collect, maintain, or disseminate the Social Security Number:					

General Personal Data (GPD)					
a. Name	✓	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	✓	c. Work Email Address	✓
d. Work Address		e. Work Telephone Number		f. Salary	
g. Employment History		h. Procurement/Contracting Records		i. Employment Performance Rating	
j. Other work-related data: Type of organization or how they are connected to museums/libraries.					

System Administration/Audit Data					
a. IP Address	✓	b. User ID/Username		c. Date/Time of Access	✓
d. Queries Run		e. ID of Files Accessed		f. Personal Identity Verification (PIV) Card	
Other system administration/audit data: Emails sent from the Granicus include single pixel gifs/ web beacons, which contain unique identifiers that enable Granicus and IMLS to recognize when their contacts have opened an email or clicked certain links.					

2.2 Indicate the source 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:	Individuals sign up for emails from IMLS via Granicus GovDelivery through www.imls.gov/news/subscribe.
Government Sources:	Professional contacts are often retrieved from the electronic Grants Management System (eGMS) where information is uploaded from official grant applications, and the individuals have consented to being contacted by IMLS.
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 within each category whose PII is contained within the system/project (including the number of minors, if any).

Members of the public	26,000 (includes professional staff, no minors)
IMLS employees/contractors	65 (no minors)
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.).

20 U.S.C. § 9103(c) (The Museum and Library Services Act of 2018 (20 USC Ch. 72))

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

Individuals can update their own information in the system. IMLS occasionally receives requests to update email addresses from individuals. Professional association lists are reviewed to ensure returned emails are accurate or if they need to be revised or removed. Individuals are also able to remove themselves from the distribution lists and due to the nature of the platform, IMLS cannot resubscribe users without their permission.

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.)	X. Certain information collected through the GovDelivery platform is subject to the Paperwork Reduction Act. That specific information is going through the process of getting clearance currently.
No.	

2.7 What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system/project?

These are temporary files. Information is deleted when superseded, obsolete, or when customer requests the agency to remove the records.

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

These are temporary files. Information is deleted when superseded, obsolete, or when customer requests the agency to remove the records.

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.).

Information collected is expressly used to maintain distribution lists for communicating important announcements, upcoming events, and funding opportunities. The GovDelivery platform allows administrators to connect with specific audiences to minimize the quantity of emails organizations receive.

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

The system collects the minimum required information for IMLS to effectively communicate with its professional audiences (name, email address, organization type). Optional information can also be provided by the individual (job title, organization demographic, interest in grants).

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.).

IMLS uses the information collected to distribute official communications from the agency to improve understanding of the organization, its activities, and potential opportunities for relevant public and professional audiences.

3.4 Does the system/project use or interconnect with any of the following technologies? (Check all that apply.)

Social Media	
Web-based Application (e.g., SharePoint)	✓
Data Aggregation/ Analytics	✓
Artificial Intelligence/ Machine Learning	
Persistent Tracking Technology	
Cloud Computing	✓
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.	Some contacts are manually pulled from the electronic Grants Management System (eGMS).
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 PII shared, purpose, and means of sharing the PII, as well as the name of the information sharing agreement.)	
No, this system/project does not connect with, obtain data from, 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 made available through it.

Members of the public	None
IMLS employees/contractors	A small group of IMLS employees

Other (explain)	

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

Yes? Explain (including what information is compiled in the log).	Systems like Granicus typically maintain audit/access logs. For example https://support.granicus.com/s/article/Granicus-LLC-SubscriberPrivacy-Statement?language=en_US provides " Granicus and its partners use cookies or similar technologies to analyze trends, administer the website, track users' movements around the website, and to gather demographic information about our user base." These logs allow IMLS to see open rates, click rates, and device used.
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 Granicus Communications Suite tools, including the FedRAMP authorized Communications Cloud marketing platform, are protected at their top-tier data centers. The data centers adhere to top certification requirements and assure that organizational data and citizen data is safe and kept private.
- Encryption: At rest encryption of all data, always.
- Security Scanning: Weekly automated scanning at the application, host, and network level by a dedicated team of security experts.
- Physical Security: Facility protected by five concentric security rings and constant monitoring of common and restricted areas.
- Archiving: High performing cache and SSD storage for archiving of video and other large files.
- Virtualized Servers: Facilitates minimal downtime for application improvements and superior failover protection
- User Account Security: Granicus has an integration with MAX.gov's MAX Authentication service, enabling organizations to utilize multi factor authentication to ensure appropriate levels of security for administrators. Using SMS messages, PIV or common access cards, federal Granicus administrators are able to further secure access to the govDelivery Communications Cloud using multiple authentication points.

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.

There are privacy risks inherent to storing information on external platforms. These risks include cyberattacks, hacks, or unauthorized access to the external partner. However, Granicus's GovDelivery Communications Cloud is the only FedRamp certified government communications tool. Please see the section above for more detailed safeguards information. Their secure environment has withstood comprehensive and rigorous review at the JAB level, approved by CIOs from the General Services Administration (GSA), the Department of Defense (DOD) and the Department of Homeland Security (DHS).

IMLS staff undergo federally required annual training on ethics and privacy.

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	☐
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.

Please see section 4.6 and 4.7.

[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." (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." (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." (Emphasis omitted). National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards Publication 199 at 2-3. (February 2004), https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf.

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):	X. Granicus has a privacy policy available on their website and also includes a consent notification during the subscription process. We will also post this PIA on our website.
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:	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:	X	
	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.

Individuals can update their own information in the system. IMLS occasionally receives requests to update email addresses from individuals. Professional association lists are reviewed to ensure returned emails are accurate or if they need to be revised or removed.

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.	☑

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.

[2] *See* Privacy Act of 1974, § 552(a)(5), https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf.

Section 7. Assessment Analysis (to be completed by OCIO and OGC)

Granicus' GovDelivery is FedRamp certified. The system does not contain information that is highly sensitive. However, the information that is contained within GovDelivery is the minimum PII required for the agency to maintain connection with our constituents and professional audiences. GovDelivery has established appropriate security controls to protect the information contained within the system (e.g., multi-factor authentication, regular password reset prompting, physical security protection, security scanning, etc.). In addition to those measures, IMLS has implemented security controls and training to ensure proper handling of the information collected through this platform.