AmeriCorps
Privacy Impact Assessment (PIA)

1- GENERAL SYSTEM INFORMATION		
1-1	**Name of the information system:**	GovDelivery Communications Cloud
1-2	**System Identifier (3 letter identifier):**	GDC
1-3	**Unique Investment Identifier (Exhibit 53):**	Contract Number 95332A22F00021
1-4	**Office or entity that owns the system:**	AmeriCorps
1-5	**Office or entity that operates the system:**	Granicus
1-6	**State if the system is operational or provide the expected launch date:**	Operational
1-7	**System's security categorization:**	Moderate
1-8	**Date of most recent Security Assessment and Authorization (SA&A) or why one is not required:**	June 24, 2024
1-9	**Approximate number of individuals with Personally Identifiable Information (PII) in the system:**	1.5 million subscribers are in the system Currently.

3- SIGNATURES (ORIGINAL MAINTAINED BY CHIEF PRIVACY OFFICER)			
	Role	***Signature***	***Date***
3-1	**Information System Owner:**		
3-2	**Office of General Counsel:**		
3-3	**Chief Privacy Officer:**		
3-4	**Chief Information Security Officer:**		
3-5	**Senior Agency Official for Privacy:**		

4- PIA HISTORY	
4-1	**State whether this is the first PIA for the system or an update to a signed PIA.**
	This is an updated PIA for the system.
4-2	**If this is an update, describe any major system changes since the last PIA. If this is the first time a PIA is being completed, write Not Applicable.**
	Not applicable
4-3 A	**State whether this is the annual review of a PIA.**
	This is an annual review.
4-3 B	**Describe any changes to the system, data activity, policies, procedures, any interrelating component and process, vendor, third parties, contracts and any required controls since last PIA.**
	This is an updated PIA due to the new collection of data from AmeriCorps Climate Change Portal.
4-3 C	**Describe objects and results of audit or tests (continuous monitoring).**
	Not applicable
4-3 D	**Certify and state "Completion of Review" if no change occurs.**
	Not applicable
4-4	**If the system is being retired, state whether a decommission plan is completed and attach a copy.**
	Not applicable

5- SYSTEM PURPOSE	
5-1	**Describe purpose of the system (or program, product, service)**
	GovDelivery is a Software as Service (SaaS) FedRAMP authorized cloud service that provides a web-based application delivered via Government Community Cloud. In order to continue to utilize a broadcast communication platform to effectively communicate with AmeriCorps' various audiences, both internally and externally, AmeriCorps procures from Granicus the GovDelivery digital communication management platform, including the Advanced and FedRAMP packages. This system has streamlined marketing capabilities that incorporate greater degrees of audience segmentation, personalization, message testing, and mobile engagement. This tool allows AmeriCorps to send email and Short Message Service (SMS) messages to multiple recipients in a strategic and controlled method, and helps AmeriCorps attain its strategic objective of recruiting members, volunteer, and grantees. AmeriCorps will use this system to seamlessly communicate with individuals, grantees, employees, members, and others to keep

		them informed of its programs and new initiatives, share inspirational stories and accomplishments, and promote member and volunteer recruitment.

6- INVENTORY OF PII		
6-1	**Provide a list of all the PII included in the system.**	
		• Name • Zip Code • Personal E-mail Address • Business E-mail Address • Phone number

7- CATEGORIES OF INDIVIDUALS IN THE SYSTEM		
7-1	**Describe the categories of individuals whose PII is in the system and state approximately how many individuals are in each category.**	
		The categories of individuals whose PII is in the system include grantees, members, and other external individuals. Currently, this system maintains approximately 1.5 million subscribers' sign-up contact information in the system.

8- INFORMATION IN THE SYSTEM		
8-1 A	**For each category of individuals discussed above: Describe the information (not just PII) collected about that category and how the information is used.**	
		The email addresses, names, phone numbers, and zip-codes are collected from the individuals who opt in to receive more information of interest from various AmeriCorps programs, via AmeriCorps website, social medical platform or AmeriCorps member and grantee portals. The information is used to establish and maintain contact with individuals through the GovDelivery system, share more information about AmeriCorps' programs, drive public engagement, analyze audience and market segmentation, and promote member and volunteer recruitment.
8-1 B	**State whether the system derives new data, or creates previously unavailable data, about an individual via aggregation of information or other means. Explain why, how it is related to the purpose of the system, how it is used, and with whom it is shared.**	
		Not Applicable
	If the system uses commercial or publicly available data, explain why, how it is related to the purpose of the system, and how it is used.	

8-1C		Not Applicable
8-1D		**Describe any application of PII redaction, mask, anonymization, or elimination.**
		The system only collects PII that is necessary. The PII is provided directly and voluntarily by individuals who opt in to receive more information of interest from various AmeriCorps program offices. The PII from external sources is transferred to GovDelivery with standard encryption. Furthermore, only AmeriCorps staff members who have been authorized and granted access to the GovDelivery system can see the PII in the system. PII is deleted when the user unsubscribes or when the user no longer hasa grant with AmeriCorps. When a user unsubscribes, the information is automatically deleted from the platform. In the case of grantees or members, the program staff managing these user lists are responsible for removing someone who is no longer a grantee, sponsor, or member.
8-1E		**Describe any design that is used to enhance privacy protection.**
		Granicus provides data privacy protection as a data processor. In addition to limiting access to only those resources that require access to the system, Granicus keeps a complete audit log of all system activities. Access is limited by role-based access and an audit log of system activity is kept for 365 days. Granicus has policies in place that include technological and organizational measures to appropriately protect the data. Granicus has identified the roles and responsibilities to ensure its management team and employees are accountable and follow its data protection requirements.

9- COLLECTIONS OF PII INTO THE SYSTEM		
9-1		**Describe for each source of PII in the system:** **a. The source.** **b. What comes from that source.** **c. How the PII enters the system.**
		The sources of PII: 1. Individuals who interact with AmeriCorps directly on AmeriCorps' websites and subscribe to receive more information from AmeriCorps. 2. Internal transfer from other AmeriCorps systems. 3. External transfer from social media platforms with consent from the individuals. 4. Individuals who interact with American Climate Corp (ACC) and subscribe to receive more ACC program information/. The PII from these sources includes name, personal email address or business email address, zip code, and phone number. In addition, the age range of the individuals who subscribe to ACC program information is collected via GovDelivery form embedded on ACC website portal

		PII can be entered into the GovDelivery system directly from an individual who voluntarily complete a subscription form on AmeriCorps' websites. The PII includes email address. PII can also be entered into the system by a system administrator in charge of uploading a grantee or member email list for their AmeriCorps program. This list is obtained from an AmeriCorps grant management system. PII can be transferred from AmeriCorps' social media ads and uploaded into GovDelivery, which includes name, email addresses, and/or zip codes. The source of personally identifiable information (PII) entered into the embedded contact form of GovDelivery on ACC is the public individuals who voluntarily complete the contact information form on the designated website. The information includes name, email address, zip code and age range.
9-2	**If any PII comes directly from the individual, describe the privacy controls in place. If all PII comes from a secondary source, write <u>Not Applicable</u>.**	
		AmeriCorps only collects and maintains PII based on individual's consent. An individual is directed to AmeriCorps privacy program webpage to review AmeriCorps' privacy policy before they decide to opt-in to voluntarily provide their contact information on the subscription form. AmeriCorps posts privacy notices on paid social media advertisements informing individuals of AmeriCorps' data collection and privacy practice and provides individuals with opt-in option before AmeriCorps collects any information from the individuals. The PII that AmeriCorps collects or receives includes only essential information required for maintaining and improving communication with the individuals, promoting recruitment of more members and volunteers and driving public engagement. AmeriCorps ensures that the transmission of PII is strictly conducted with required encryption method. The information is secured by GovDelivery system with a series of information security and privacy control measures that the service provider is required to implement.
9-3	**If PII about an individual comes from a secondary source other than the individual, describe:** **a. Why the PII is collected from the secondary source.** **b. Why the PII from the secondary source is sufficiently accurate.** **c. If/how the individual is aware that the secondary source will provide their PII.** **If all PII about an individual comes directly from the individual, write <u>Not Applicable</u>.**	

		Not applicable.
9-4	**If any collections into the system are subject to the Paperwork Reduction Act (PRA), identify the Office of Management and Budget (OMB) Control Number for the collection and effective date. If the system does not implicate the PRA, write Not Applicable.**	
		Not applicable
9-5	**If any collections into the system are subject to an agreement, describe those agreements. If no agreements are relevant, write Not Applicable.**	
		AmeriCorps has signed partnership agreements with other partner agencies which would allow sharing of GovDelivery website link to more audience for the purpose of promoting partnership programs that AmeriCorps executes. The new audience might choose to enter their subscriber information into the forms hosted by GovDelivery.

10- SYSTEM ACCESS		
10-1	**Separately describe each category of individuals who can access the system along with:** **a. What PII they can access (all or what subset).** **b. Why they need that level of access.** **c. How they would request and receive that access.** **d. How their access is reduced or eliminated when no longer necessary.** **e. Identify policies and procedure outlining roles and responsibilities and auditing processes.**	
		AmeriCorps employees who work as administrators responsible for crafting messages for grantees, members, or external audiences and updating subscription lists have authorized access to GovDelivery and can see the PII present in the system. They need full access to manage subscriptions, and to send emails to subscribers. The information that is emailed to subscribers is related to grant changes, new policies for grantees and members, invitations to trainings and other events, and general AmeriCorps information about various programs and services. AmeriCorps staff request access through the Office Communication and Marketings team and must successfully complete required training before their account is created and access is granted. The account access list is reviewed and updated monthly by the system owner. In the event an employee is no longer a part of the AmeriCorps staff or does not require access to the GovDelivery system due to a change in their role or duties, the system owner will delete the account. There are currently 78 AmeriCorps employees who have access to the GovDelivery system.

11- PII SHARING		
11-1	**Separately describe each entity that receives PII from the system and:** **a. What PII is shared.** **b. Why PII is shared** *(specify the purpose)* **c. How the PII is shared (what means/medium).**	

	d. The privacy controls to protect the PII while in transit. **e. The privacy controls to protect the PII once received.** **f. PII sharing agreements (***describe if the agreement specifies the scope of the information sharing, the parties to the agreement, and the duration of the agreement***)** **g. Describe security and privacy clauses and audit clauses in the agreement or vendor (including third party vendors) contract.** **If PII is not shared outside the system, write Not Applicable.**
	Not Applicable.

12- PRIVACY ACT REQUIREMENTS	
12-1	**If the system creates one or more systems of records under the Privacy Act of 1974:** **a. Describe the retrieval that creates each system of records.** **b. State which authorities authorize each system of records.** **c. State which system of records notices (SORNs) apply to each system of records.** **If the system does not create a system of records, write Not Applicable.**
	The records in the system can be retrieved by email address or full text. This system of records is authorized by the National and Community Service Act of 1990, as amended (42 U.S.C. chapter 129), the Domestic Volunteer Service Act of 1973, as amended (42 U.S.C. chapter 66); and Executive Order 13571. The applicable SORN is CNCS–05–OEA–SNPE Social Network and Public Engagement System of Records [88 FR 30728].

13- SAFEGUARDS	
13-1	**Describe the data processing environments and the technical, physical, and administrative safeguards (including vendors') that protect the PII in the system.**
	The vendor Granicus is responsible for providing majority of the technical, physical, and administrative safeguards to protect the PII within AmeriCorps GovDelivery account. Regarding the administrative safeguards, Granicus and AmeriCorps both require that all employees and contractors complete a few mandatory trainings upon hire and annually to be granted access to GovDelivery. The trainings that must be completed are the Acceptable Use Policy Training (includes handling of customer data), Security Awareness Training, Privacy Training, and Insider Threat Training. Additional trainings that may be required based upon certain roles and responsibilities are Incident Response Training, Contingency Plan Training, Role-based training, and other ad hoc trainings. Last, Granicus and AmeriCorps require all employees and contractors to review and agree to abide by the Rules of Behavior (ROB), Confidentiality, and Non-Disclosure agreements via signature.

		GovDelivery collects and stores data electronically. Use of FIPS-140-2 encryption is mandatory to protect all GovDelivery data at rest and in transit. Access to GovDelivery data is limited to role-based access controls and the principle of least privilege. Furthermore, a user can only gain access to the system (i.e., username, password, pin) after successfully passing two-factor authentication. Granicus and AmeriCorps implemented and follow all required access control requirements for GovDelivery system. Breach response and data spillage are core components with AmeriCorps's incident response plan and procedures. Data is backed up only through replication within AmeriCorps security boundary. Removable media is not allowed within data centers. The use of removable media requires Granicus employees to follow proper protections for the management and disposal of removable media in conformance with AmeriCorps Information Classification and Handling Standard. Log data is protected while managed and properly destroyed after use per media protections requirements. The PII that are subject to disposition would be appropriately destroyed per the Information Classification and Handling Standard associated with GovDelivery.
13-2	**Describe the technical, physical, and administrative measures that protect PII if the system is being retired.**	
		Not applicable
13-3	**State if a system security plan and privacy plan is completed and the date of control verification.**	
		The System Security and Privacy Plan was completed and approved on July 24, 2024.

14- DATA ACCURACY, ACCESS, AMENDMENT, AND CONTROL		
14-1	**Describe the steps taken to ensure PII is sufficiently accurate, relevant, current, and complete, as well as the assurance procedure.**	
		PII is provided by the individual voluntarily.
14-2	**Describe how an individual could view, correct, update, or ask to amend their PII.**	
		After the individual submit their PII via the subscription form, they cannot see or edit the PII. Individuals can reference their email subscription confirmation email for details on the PII he/she has provided. However, they can correct, update or amend their PII by unsubscribing and then completing a new subscription.
14-3	**Describe how an individual could control what PII about themselves is included in the system or how it is used. Also describe how those decisions could affect the individual.**	
		For the individuals who provide PII via the subscription from, they can cancel their subscription at any time, which would remove their PII permanently. Removal of the PII will not negatively affect an individual.
14-4	**State if PII handling processes apply automation technology for decision making and describe the measures taken to eliminate risk to privacy interests.**	
		Not Applicable.

15- DATA RETENTION AND DESTRUCTION	
15-1	**Identify the National Archives and Records Administration (NARA) provided retention schedule for the system and provide a summary of that schedule.**
	The records are retained indefinitely until they are scheduled with the National Archives and Records Administration and are eligible for disposition under those schedules. The Record Schedule Request form has been completed, and the NARA retention schedule will be provided in the near future.
15-1	**Identify the role and process to coordinate with the parties involved in record retention and disposition.**
	Upon official review and completion of the Record Schedule Request form, these details will be determined and identified.

16- SOCIAL SECURITY NUMBERS (SSNs)	
16-1	**If the system collects truncated or full social security numbers (SSNs):** **a. Explain why the SSNs are required.** **b. Provide the legal authority for the usage of the SSNs.** **c. Describe any plans to reduce the number of SSNs.** **If the system does not collect any part of an SSN, write Not Applicable.**
	Not Applicable.

17- WEBSITES	
17-1	**If the system includes a website which is available to individuals apart from AmeriCorps personnel and contractors, discuss how it meets all AmeriCorps and Federal privacy requirements. If the system does not include a website, write Not Applicable.**
	• AmeriCorps does not endorse any third-party websites; notices are provided when there is a link to a third-party website. • AmeriCorps privacy policy is clearly shown on the website, there is a highlighted link that all subscribers are required to acknowledge during the initial request for subscription. The website address is as follows: https://public.govdelivery.com/accounts/USCNCS/subscriber/new

18- OTHER PRIVACY RISKS	
18-1	**Discuss any other system privacy risks or write Not Applicable.**
	Not Applicable.