AmeriCorps
Privacy Impact Assessment (PIA)

1- GENERAL SYSTEM INFORMATION		
1-1	**Name of the information system:**	Everbridge Suite
1-2	**System Identifier (3 letter identifier):**	
1-3	**Unique Investment Identifier (Exhibit 53):**	
1-4	**Office or entity that owns the system:**	Office of Facilities and Support Services (OFSS)
1-5	**Office or entity that operates the system:**	Everbridge, Inc.
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:**	Initial Assessment
1-9	**Approximate number of individuals with Personal Identifiable Information (PII) in the system:**	The contact information of approximately 524 AmeriCorps staff is maintained in the system.

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:**		

AmeriCorps

4- PIA HISTORY	
4-1	**State whether this is the first PIA for the system or an update to a signed PIA.**
	This is the first 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 PIA.**
	No
4-3 B	**Describe any changes to the system, data activity, policies, procedures, any interrelating component and process, vendor, 3rd parties, contracts, and any required controls since last PIA.**
	No changes documented.
4-3 C	**Describe objects and results of audit or tests (continuous monitoring).**
	No audits or tests have been conducted yet.
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)**
	Everbridge Suite (EBS) is a Software-as-a-Service platform that is used for managing critical events. AmeriCorps procures EBS from Everbridge Inc. and uses the EBS platform for operational response to critical events, to keep people safe, and to maintain business continuity. During public safety threats, severe weather conditions, and critical business events (such as IT outages or cyber-attacks), AmeriCorps relies on the EBS platform to quickly and reliably execute predefined communications processes and to track progress on executing incident response plans. The EBS services used include Everbridge Mass Notification and Everbridge ManageBridge. Everbridge Mass Notification allows administrators to send notifications to individuals or groups using lists and locations. Everbridge Mass Notification is supported by state-of-the-art security protocols, elastic infrastructure, advanced

		mobility, interactive reporting and analytics, adaptive people and resource mapping to mirror AmeriCorps' organization, and true enterprise class data management capabilities to provide a wide array of data. The Everbridge ManageBridge is a mobile application solely used by AmeriCorps administrators, allowing them to execute communications from anywhere in an emergency situation when administrators are away from the full desktop application. AmeriCorps contractors who are on-site will be contacted via Teams. AmeriCorps employees and contractors will be contacted via contact information that they provide to EBS.

6- INVENTORY OF PII		
6-1	**Provide a list of all the PII included in the system.**	
		The Everbridge system collects PII such as first name, middle initial, last name, and AmeriCorps business contact information. ○ First Name ○ Middle Initial ○ Last Name ○ Location (Office location – city/state) ○ Business Phone Number ○ Business Email Address Users may elect to input the following personal information into the system to receive emergency notifications from AmeriCorps: ○ Personal Phone Number ○ Personal Email Address

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 category of individuals whose PII is in the system includes AmeriCorps staff and on-site contractors, which is approximately 524 individuals.

8- INFORMATION IN THE SYSTEM	
	For each category of individuals discussed above:

8-1 A	**Describe the information (not just PII) collected about that category and how the information is used.**
	The Everbridge system is used by AmeriCorps for sending emergency notifications. The purpose of collecting contact information of AmeriCorps staff is to distribute messages, recordings or alerts during an emergency or incident whereby notifications will need to be sent to the impacted audience. The purpose of collecting administrative users' names and business contact information is to process and authorize their access to the system to send notifications to all AmeriCorps employee and contractors.
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. The system does not derive new data, or create previously unavailable data, about an individual via aggregation of information or other means.
8-1 C	**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.**
	Not Applicable. Everbridge does not use publicly available data.
8-1 D	**Describe any application of PII redaction, mask, anonymization, or elimination.**
	There is no PII redaction, masking anonymization or elimination.
8-1 E	**Describe any design that is used to enhance privacy protection.**
	Everbridge Suite has been certified under ISO 27701, General Data Protection Regulation (GDPR), and Cloud Computing Compliance Controls Catalog (C5).

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 source of PII is AmeriCorps' official staff directory to include the below business contact information: ○ First Name ○ Middle Initial ○ Last Name ○ Location (Office location – city/state)

		○ Business Phone Number ○ Business Email Address When AmeriCorps Everbridge administrators receive notification of an employee or contractor onboarding, the administrator manually creates a new account for the user and inputs the above information into the system. The user is then invited to create a login to the Everbridge system to verify the business contact information, determine order for receipt of their notifications (business email address, text, and/or voicemail), and optionally, add in additional PII noted below. The second source of PII is from employees and contractors who optionally elect to populate the system with their personal phone number and/or email address during the account creation portion.
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>.**	
		All new employees and contractors receive a welcome invitation from the Everbridge system upon onboarding. The registration is mandatory. The registration invitation provides information to the users on what the system is and how to register/create an account with Everbridge. All non-business PII is entered manually into the Everbridge system by AmeriCorps employees and contractors themselves during the account creation and management process. All AmeriCorps Everbridge Administrators that are granted permission to the Everbridge system have minimum background investigation (MBI) clearance. Access logs are available for auditing. The failed login attempts are set to a maximum number and continued failed attempts to login will result in being locked out/denied access until the account access for that user is unlocked by a system administrator. Only AmeriCorps system administrators are authorized to manually enter PII obtained from AmeriCorps' official staff directory which has secured connection and encryption controls in place to protect the PII at rest and in transit. Access into the Everbridge system is secured by Multifactor Authentication and Virtual Private Network (VPN).
9-3	**If PII about an individual comes from a 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>.	
		Primary source for PII is from AmeriCorps' official staff directory and is collected to ensure that at a minimum, all employees and contractors receive critical information during an emergency. Employees are aware of this primary source via their introductory invitation to register with the system and on the system login page.
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 <u>Not Applicable</u>.**	
		Not Applicable
9-5	**If any collections into the system are subject to an agreement, describe those agreements. If no agreements are relevant, write <u>Not Applicable</u>.**	
		Not Applicable

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 staff and on-site contractors can access their own PII information (business and personal phone number or email address if they elected to include it) in Everbridge, without any restrictions. Account access is through the Everbridge application, where users can also delete or update their PII. Users are invited to access Everbridge via an invitation from the AmeriCorps Everbridge administrators. Access is eliminated by the administrators when the employee or contractor terminates from AmeriCorps. Everbridge administrators can delete accounts, which will remove all employee or contractor PII from the 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, parties of 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 <u>Not Applicable</u>.**	
		Not Applicable. PII is not shared outside of the Everbridge application.

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 SORNs apply to each system of records.** **If the system does not create a system of records, write <u>Not Applicable</u>.**	
		The record can be retrieved by name. The legal authorities that authorize this system of records include: Federal Continuity Directive 1, Federal Executive Branch National Continuity Program and Requirements, January 17, 2017; Federal Property Management Regulation (FPMR) 101-20.103-4, Occupant Emergency Program; Homeland Security Presidential Directive 20, National Continuity Policy, May 4, 2007. The applicable SORN is CNCS-20-COO-ERC Emergency Response System of Records, pending publication.

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 information in the Everbridge database is protected from misuse and unauthorized access through various administrative, technical, and physical security measures consistent with statutory and regulatory prohibitions on misusing confidential information. Technical security measures within AmeriCorps include restrictions on computer access to authorized individuals, required use of PIV for identity and

		authentication, the use of encryption for certain information types and transfers, and regular review of security procedures and best practices to enhance security. Physical measures include restrictions on building access to authorized individuals and maintenance of records in lockable offices and filing cabinets. AmeriCorps employees and contractors who are off-site may access the AmeriCorps corporate network outside the firewall via a secure Cisco AnyConnect VPN. Other data security and privacy protection controls and measures that the vendor of Everbridge Suite FedRAMP has put in place cover: • Breach response policy and procedure. • Data backups, removable media, and hard copy data. • Rules of behavior, confidentiality agreements, or non-disclosure agreements. • Encryption in transit and at rest. • The creation and review of any audit logs.
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.**	
		AmeriCorps System Security Plan is still being developed and estimated to be completed by June 2024.

14- DATA ACCURACY, ACCESS, AMENDMENT, AND CONTROL		
14-1	**Describe the steps taken to ensure PII is sufficiently accurate, relevant, current, and complete and the assurance procedure.**	
		The information that is in Everbridge comes directly from AmeriCorps' official staff directory and/or directly from employees and contractors themselves.
14-2	**Describe how an individual could view, correct, update, or ask to amend their PII.**	
		All AmeriCorps employees and contractors must update, correct, and amend their own PII if it changes during their employment at the agency.
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.**	

	The only field available for AmeriCorps employees and contractors are following: ○ First Name ○ Middle Initial ○ Last Name ○ Location (Office location – city/state) ○ Business Phone Number ○ Business Email Address ○ Personal Phone Number (Optional from employee) ○ Personal Email Address (Optional from employee) No additional information is accepted into the system. Individual employee and contractors must update, correct, and amend their own PII if it changes during their employment at the agency.
14-4	**State if PII handling processes apply automation technology for decision making and describe the measures taken to eliminate risk to privacy interests.**
	No, there is no automation used for handling or processing PII in Everbridge Suite.

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.**
	Everbridge is covered under General Record Schedule GRS 5.3. item 20. The disposition is temporary, and records will be destroyed when superseded or obsolete, or upon separation or transfer of employee. The Disposition Authority is DAA-GRS-2016-0004-0002.
15-2	**Identify the role and process to coordinate with the parties involved the record retention and disposition.**
	System Owner/Information System Owner will coordinate the record retention activities with the Records Retention Officer and AmeriCorps Everbridge Administrators.

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 <u>Not Applicable</u>.
	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 <u>Not Applicable</u>.**
	Not Applicable

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