AmeriCorps
Privacy Impact Assessment (PIA)

1- GENERAL SYSTEM INFORMATION		
1-1	**Name of the information system:**	AmeriCorps General Support System (GSS)
1-2	**System Identifier (3 letter identifier):**	GSS
1-3	**Unique Investment Identifier (Exhibit 53):**	485-000000014
1-4	**Office or entity that owns the system:**	AmeriCorps Office of Information Technology
1-5	**Office or entity that manages the system:**	GDIT eITS Contract
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:**	10/01/2022
1-9	**Approximate number of individuals with PII in the system:**	The GSS is AmeriCorps' primary IT infrastructure that include computers, network, several servers, and some common workplace software. GSS supports various systems and applications. These systems and applications might handle PII, of over a million individuals.

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 update to an existing system with a prior signed PIA.
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 <u>Not Applicable</u>.**	
		Major changes to the GSS since the last PIA was signed include: • New contract information • Removal of the system's connections to some external sources

5- SYSTEM PURPOSE

5-1	**Describe the purpose of the system.**	
		AmeriCorps is the Federal agency that leads service, volunteering, and grant-making efforts in the United States. The AmeriCorps General Support System (GSS) is an infrastructure system that integrates voice, video, and data as well as security and application intelligence and provides network services and general automated data processing and support for AmeriCorps. GSS includes essential hardware and network components, information security support as well as the mobile device management and Voice over Internet Protocol (VOIP) telephone service. GSS not only hosts or provides connectivity for AmeriCorps' major applications but also supports these minor applications as part of the AmeriCorps' information technology that employs various managed services in a private cloud. The GSS currently utilizes tools used to operate and secure GSS services and other common workplace software as listed below: • Intrusion Detection software • Data Loss Protection DLP service used in Microsoft SharePoint Online and OneDrive to limit the chance of an unintentional disclosure

- Microsoft 365, with applications such as Outlook, Teams, Microsoft Phone System, SharePoint Online, and OneDrive with cloud storage
- Azure Active Directory
- Tools used to send encrypted emails, such as Microsoft Outlook Encryption.
- Software that captures and correlates audit logs for most AmeriCorps systems.

6- INVENTORY OF PII

6-1 Provide a list of all the PII included in the system.

The systems and applications that GSS supports and the software components operating and securing GSS may handle PII. The VOIP telephone service, mobile device management and Microsoft Team applications in GSS might record the phone number, the time of the call, and the voicemail. Microsoft Teams may capture the caller's ID, which may also include names. Microsoft Office 365 might store some information existing in a defined and structure format with specific fields such as the names, email addresses, job titles, phone numbers for internal use. The audit log may capture events with information of username, IP address, time of access, and activities to safeguard AmeriCorps' information and asset. AmeriCorps' OneDrive online cloud storage has been used to store documentation of the activities conducted by AmeriCorps' offices and entities, which might contain PII collected from the public.

When a system or application of AmeriCorps collects PII from the public individuals, a corresponding separate PIA is or will be conducted to appropriately notify the public of AmeriCorps' PII handling activities and the data privacy safeguarding measures that AmeriCorps implements. For more information of the PII that AmeriCorps handles in general, please visit https://www.americorps.gov/privacy.

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.

GSS provides general support service to the systems and applications that might handle PII. Some of applications that GSS uses might handle PII. The PII, such as the IP addresses or phone numbers or names, can be from anyone who either has an AmeriCorps network connection, or communicates with AmeriCorps, or is a visitor to AmeriCorps' website. They can be public individuals, AmeriCorps staffs,

		AmeriCorps' service members, AmeriCorps' volunteers, or AmeriCorps' grantees, etc. The total numbers can be over one million at any time. For detailed information of the PII handled by AmeriCorps, please review the Privacy Impact Assessments and the System of Records Notices posted on Privacy Policy | AmeriCorps.

8- INFORMATION IN THE SYSTEM		
8-1	**For each category of individuals discussed above:** **a. Describe the information (not just PII) collected about that category.** **b. Give specific details about any PII that is collected.** **c. Describe how the information is used.**	
		The GSS is designed to handle electronic information and provide network service as a general support system. Its email service application might process the email to AmeriCorps and deliver response from AmeriCorps for general communication purpose, the email recipients and senders may include public individuals, AmeriCorps staffs, AmeriCorps' service members, AmeriCorps' volunteers, or AmeriCorps' grantees, etc. For the purpose of monitoring and securing the website and AmeriCorps information and systems, the audit logs may capture AmeriCorps' website visitors' IP addresses and a list of the webpages they viewed, and captures events with information of username, IP address, time of access, and activities. The VOIP and other mobile management device in GSS might record the phone number, the time of the call, and the voicemail to properly carry out the functions of the systems. Microsoft Teams may capture the caller's ID, which may also include names. Microsoft Office 365 might store some information existing in a defined and structure format with specific fields such as the names, email addresses, job titles, phone numbers for general office communication. To conduct federal business activities, AmeriCorps' offices and entities may use OneDrive to store documentation which might contain PII, yet most of the information is in a less structured format. The use of the information and the PII are described in the PIA of the systems and applications supported by GSS. This GSS PIA also provides details of the information that GSS may handle and how the information is used.

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.**

	GSS transmits information and provides general infrastructure service to the systems and applications of AmeriCorps which might handle PII. Further information about AmeriCorps systems and the PII they collect can be found in the PIAs located at Privacy Policy | AmeriCorps. The sources of the information including PII processed by the telecommunication applications, Microsoft 365 email application, Team, and other software used to operate and secure GSS can be from any users who use or access AmeriCorps' system or application, visit AmeriCorps' websites or communicate with AmeriCorps staffs. The information is documented or captured by this application by following configuration policy of AmeriCorps.
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>.**
	GSS transmits information and provides general infrastructure service to support the systems and applications of AmeriCorps which might collect PII. Further information about AmeriCorps privacy practice can be found at Privacy Policy | AmeriCorps.
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>.**
	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. 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.

The access to the system is controlled based on need-to-know and least privilege principles. The Microsoft 365 account holder might have access to the information that might contain PII to accomplish their assigned role. For example, AmeriCorps employees with the Microsoft 365 eDiscovery Managers role may execute eDiscovery searches of Microsoft 365. The controls implemented in GSS assure that each GSS Account Holder receives the appropriate levels of access to the systems and information and loses that access when no longer needed, based on the Privileged accounts roles matrix for GSS.

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.
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. Any agreements controlling that PII.

If PII is not shared outside the system, write Not Applicable.

GSS does not share PII with other systems. It provides general supports to other AmeriCorps systems and applications. Information can be transmitted through GSS.

As a standard practice, AmeriCorps does have some baseline requirements for PII sharing among the systems and applications that GSS supports or between AmeriCorps' internal system and external system, including:

- Any sharing of PII must comply with AmeriCorps Cybersecurity Policy, Privacy Policy, Data Sharing Policy, and other internal policies.
- If PII goes from one AmeriCorps system across the GSS to a third party, the PIA for the AmeriCorps system which provides the PII should describe the connection including what PII is transferred and the controls protecting that transfer.
- If the PII is from a system of records, AmeriCorps must discuss the sharing of that PII in one of the System of Records Notices (SORNs) that is or will be published in the Federal Register and posted to Privacy Policy | AmeriCorps.

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 Not Applicable.**
	Not Applicable

13- SAFEGUARDS	
13-1	**Describe the technical, physical, and administrative safeguards that protect the PII in the system.**
	GSS provides general supports to other AmeriCorps systems and applications. Information can be transmitted through GSS. To ensure that GSS provides secure infrastructure service environment, multiple levels of technical, physical, and administrative safeguards are implemented in GSS, which include but not limited to (1) Owners of folders on the "Shared" drive have the ability to request or deny access to individuals in the AmeriCorps as they sees fit. This would allow the owners to control who has access to the documents and information based on their job responsibilities and duties. (2) Information that may be restricted in some manner e.g., PII, might require the use of IP Switch Outlook Message Encryption (OME). This was implemented to assist users that are required to work with PII data. OME delivers encrypted HTTPS, FTPS/TLS, AS2, AS3 transfer methods or the secure SSH2 encrypted SFTP/SCP2 transfer methods. All data uploaded to OME is carefully protected using its built-in, FIPS 140-2 validated, AES-256 storage encryption. (3) Microsoft 365 Data Loss Prevention used automated detection to prevent sharing of SharePoint Online and OneDrive PII with external users. (4) Active Directory Group Policy requires removeable media to be encrypted when writing data (excludes optical discs). (5) Access to AmeriCorps shared resources must be approved by the AmeriCorps information system owner. The process of tracking and approving access to the resources is tracked using a ServiceNow ticket. GSS is categorized as a system with moderate risk level. The data protection controls implemented are commensurate with the identified risk level, compatible with what is required to protect the information of the systems and applications that GSS supports. The security and privacy measures including timely assessment, corrections and trainings and other control mechanisms that AmeriCorps has put

		into place are subject to continuous monitoring to ensure the assurance level can be adequately maintained.

14- DATA ACCURACY, ACCESS, AMENDMENT, AND CONTROL		
14-1	**Describe the steps taken to ensure PII is sufficiently accurate, relevant, current, and complete.**	
		AmeriCorps works to develop purpose-built collection forms to obtain accurate and complete PII through instructions, data validation checks, and other techniques. Individuals then generally have the option to access their data and update anything which is inaccurate or incomplete. The PIAs, SORN, and other documents written to describe AmeriCorps' systems that GSS supports further explain these systems and how they work to confirm the accuracy of the PII they collect. Please visit Privacy Policy | AmeriCorps for more information.
14-2	**Describe how an individual could view, correct, update, or ask to amend their PII.**	
		GSS is not a Privacy Act System. Any individual with questions about their PII in a specific privacy act system covered by a system of records notice may contact AmeriCorps privacy office via the email address posted AmeriCorps' website. For more information about the specific system that handle their PII, please visit AmeriCorps' privacy webpages.
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.**	
		GSS is used to provide general support to AmeriCorps's systems and applications which might handle PII. In almost all situations, individuals can choose whether they want to continue visiting AmeriCorps' website after they review AmeriCorps privacy policy, choose not to continue accessing AmeriCorps' network after they review the content of the government warning banner, or choose not to provide their basic contact information for email respondence when they communicate with AmeriCorps.

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.**	
		Different retention schedules apply to the records in the GSS depending on the type of records, its usage, the source, and other factors. If a schedule has been determined for a type of records, it will be disposed of according to that schedule. If not, the records will be retained until the schedule has been created and then

		disposed of according to that schedule. The disposal is conducted per the requirements of AmeriCorps Property Management Policy No.500.

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