



## AmeriCorps Privacy Impact Assessment (PIA)

1- GENERAL SYSTEM INFORMATION		
1-1	Name of the information system:	AmeriCorps Grantee and Sponsor Portal
1-2	System Identifier (3 letter identifier):	GSP
1-3	Unique Investment Identifier (Exhibit 53):	EYGA
1-4	Office or entity that owns the system:	AmeriCorps
1-5	Office or entity that manages the system:	Ernst & Young LLC
1-6	State if the system is operational or provide the expected launch date:	January 29, 2024
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:	New System currently pursuing an Authority to Operate (ATO).
1-9	Approximate number of individuals with PII in the system:	10,800. AmeriCorps anticipates that approximately 400 staff, 400 external reviewers, and up to 10,000 applicants and award recipients will use the new system annually.

250 E Street SW

Washington, D.C. 20525

202-606-5000/ 800-942-2677



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

<b>4- PIA HISTORY</b>	
<b>4-1</b>	<b>State whether this is the first PIA for the system or an update to a signed PIA.</b>
	This is the first PIA.
<b>4-2</b>	<b>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>.</b>
	Not Applicable.
<b>4-3 A</b>	<b>State whether this is the annual review of PIA.</b>
	Not an annual review, it is the initial PIA for this system.
<b>4-3 B</b>	<b>Describe any changes to the system, data activity, policies, procedures, any interrelating component and process, vendor, 3<sup>rd</sup> parties, contracts and any required controls since last PIA.</b>
	Not Applicable.
<b>4-3 C</b>	<b>Describe objects and results of audit or tests (continuous monitoring).</b>
	Not Applicable.
<b>4-3 D</b>	<b>Certify and state “Completion of Review” if no change occurs.</b>
	Not Applicable.
<b>4-4</b>	<b>If the system is being retired, state whether a decommission plan is completed and attach a copy.</b>



	Not Applicable.
--	-----------------

## 5- SYSTEM PURPOSE

<b>5-1</b>	<b>Describe the purpose of the system.</b>
	<p>The Grantee and Sponsor Portal (GSP) is a Software as a Service (SaaS) solution provided by Ernst &amp; Young LLP (EY) to replace AmeriCorps' legacy grants management system (eGrants). Grantee and Sponsor Portal serves as a single source of system for AmeriCorps to manage programs and opportunities. AmeriCorps will use GSP to enable the collection and review of applications, and the issuance and monitoring of performance and costing of any subsequent awards or sponsor agreements. Grantee and Sponsor Portal will integrate with AmeriCorps' data hub and federal government systems such as SAM.gov, Login.gov, Grants.gov, Treasury ARC (Oracle Federal Financials), and the Payment Management System (PMS) of the Department of Health and Human Services. Information from this system may be shared with other AmeriCorps or Federal systems to complete any public reporting or evaluations required by law, regulations, and/or executive orders.</p>

## 6- INVENTORY OF PII

<b>6-1</b>	<b>Provide a list of all the PII included in the system.</b>
	<ul style="list-style-type: none"> <li>• Name (including nicknames)</li> <li>• Group/Organization Membership</li> <li>• Organization Name</li> <li>• Employer Identification Number (EIN)</li> <li>• Business Email Address</li> <li>• Business Mailing Address</li> <li>• Business Phone Number</li> </ul>

## 7- CATEGORIES OF INDIVIDUALS IN THE SYSTEM

<b>7-1</b>	<b>Describe the categories of individuals whose PII is in the system and state approximately how many individuals are in each category.</b>
	<p>1) Individuals who handle award applications and manage award for the partner organizations applying for or receiving grant funds or people power resources from AmeriCorps: approximately 10,000 annual users fall into this category.</p>



	<p>2) AmeriCorps contractors assist AmeriCorps staff with award monitoring activities, providing training or technical assistance to applicants or award recipients, providing system operations, maintenance, and security support. External Reviewers will receive and review applications and related materials (e.g., evidence documentation). They will document review results and engage with review panel and agency staff. There are approximately 400 annual users fall into this category.</p> <p>3) AmeriCorps staff reviewing applications and monitoring awards: approximately 400 users.</p>
--	---

8- INFORMATION IN THE SYSTEM	
8-1 A	<p><b>For each category of individuals discussed above:</b></p> <ol style="list-style-type: none"> <li><b>Describe the information (not just PII) collected about that category.</b></li> <li><b>Give specific details about any PII that is collected.</b></li> <li><b>Describe how the information is used.</b></li> </ol> <p>Individuals who handle award applications and manage award for an organization applying for or receiving AmeriCorps resources will input their names, organization affiliation information, business email addresses, and business phone numbers. This information is used to enable these individuals to establish and maintain accounts within the Grantee and Sponsor Portal so as to submit applications or manage awards on behalf of organizations. AmeriCorps will use this information to contact these individuals in reference to the applications or awards they submitted in the system.</p> <p>The names, business email address, and business phone numbers of AmeriCorps' contractor and external reviewer are entered into the Grantee and Sponsor Portal so that they can be provided with appropriate access to the system to perform activities in accordance with their specific roles and or contractual requirements.</p>
8-1 B	<p><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.</b></p> <p>Not Applicable.</p>
8-1 C	<p><b>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.</b></p>



	Not Applicable.
8-1 D	<b>Describe any application of PII redaction, mask, anonymization or elimination.</b>
	The Grantee and Sponsor Portal enables "Field Level Security" that can mask certain fields with symbols and characters to conceal information. The access to the data is role-based with specific restriction.
8-1 E	<b>Describe any design that is used to enhance privacy protection.</b>
	Annual checks will ensure PII information is reviewed for eligibility, then deleted appropriately. The Microsoft Power Platform that GSP utilizes also has full auditing of user actions. The system is hosted on an Enclave of Ernst & Young Government and Public Sector (EY GPS), which is built on the Microsoft Azure Gov (Virginia) Cloud platform and is Government Community Cloud High Compliant. The environment is protected with Azure Firewall services, and logs are monitored with Azure Log Analytics. The Ernst and Young Grants Accelerator (EYGA) architecture features a Backup Resource Group for data backups and system redundancy (Vault, Storage Account Backup Containers, and Recovery Services Vault). Data in transit is encrypted with TLS 1.3 HTTPS connections. Microsoft Azure Defender is configured to protect the environment.

9- COLLECTIONS OF PII INTO THE SYSTEM	
9-1	<b>Describe for each source of PII in the system:</b> a. <b>The source.</b> b. <b>What comes from that source.</b> c. <b>How the PII enters the system.</b>
	<p>For the individual users working for an organization applying for AmeriCorps resources, they will enter their name and other business contact information directly into the Grantee and Sponsor Portal at the time they establish their user account. Persons with account administration privileges in the Grantee and Sponsor Portal will also be able to invite other individuals from their organization to access the Grantee and Sponsor Portal, who will enter their names, business email addresses, and business phone numbers. This information is entered into the system through manual data entry as part of the user account set-up. The Grantee and Sponsor organizations self-manage access to their accounts in this system. The organization's account administrator(s) can invite and otherwise manage accounts based on their organization's internal policy and procedures. Each organization can have multiple staff who are able to view and enter applications for projects or report on existing awards.</p> <p>The name of the contractors, external reviewers and AmeriCorps staffs will provide their names along with their business contact information for setting up account so as to access the system to perform their job duties.</p>



9-2	<p><b>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>.</b></p> <p>There is a banner on the login page of this system website which describes the purpose of the system and warns that the system is government-owned, and all the user activities are being monitored. To use the system for grant application and award management purpose, the individuals who apply for and manage awards for an organization would be prompted to provide their names, organization email addresses, and organization phone numbers.</p> <p>All the public facing websites of AmeriCorps have direct link to the privacy policy and privacy program webpages of AmeriCorps which inform the website visitors of the privacy practice of AmeriCorps.</p>
9-3	<p><b>If PII about an individual comes from a source other than the individual, describe:</b></p> <ol style="list-style-type: none"> <li><b>Why the PII is collected from the secondary source.</b></li> <li><b>Why the PII from the secondary source is sufficiently accurate.</b></li> <li><b>If/how the individual is aware that the secondary source will provide their PII.</b></li> </ol> <p><b>If all PII about an individual comes directly from the individual, write <u>Not Applicable</u>.</b></p> <p>Not Applicable.</p>
9-4	<p><b>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>.</b></p> <p>Information collected in the Grantee and Sponsor Portal is currently covered by the following OMB Control Numbers:</p> <ul style="list-style-type: none"> <li>• 3045-0010 (09/30/2025) NCCC</li> <li>• 3045-0035 (11/30/2024) Seniors</li> <li>• 3045-0038 (05/31/2024) VISTA</li> <li>• 3045-0047 (09/30/2023) ASN Apps</li> <li>• 3045-0099 (02/29/2024) Commission Support</li> <li>• 3045-0102 (09/30/2024) OFMS</li> <li>• 3045-0180 (03/31/2026) DOS</li> <li>• 3045-0184 (12/31/2025) ASN PPRs</li> <li>• 3045-0187 (10/31/2023) Generic Grant Application</li> <li>• 4040-0004 (11/30/2025) SF-424</li> <li>• 4040-0006 (02/28/2025) SF-424A</li> <li>• 4040-0007 (02/28/2025) SF-424B</li> <li>• 4040-0014 (02/28/2025) SF-425</li> </ul>



<b>9-5</b>	<b>If any collections into the system are subject to an agreement, describe those agreements. If no agreements are relevant, write <u>Not Applicable</u>.</b>
	Not Applicable.

## 10- SYSTEM ACCESS

<b>10-1</b>	<b>Separately describe each category of individuals who can access the system along with:</b> <b>a. What PII they can access (all or what subset).</b> <b>b. Why they need that level of access.</b> <b>c. How they would request and receive that access.</b> <b>d. How their access is reduced or eliminated when no longer necessary.</b>
-------------	--

	<p>Administrator team:</p> <ol style="list-style-type: none"> <li>They can view and access all PII provided by the applicant.</li> <li>They need this access to provide enhancements and issue patches/fixes and to triage incidents and perform service desk support.</li> <li>Administrators may grant access to the system to additional administrators/developers as needed.</li> <li>Access can be manually changed or removed as necessary.</li> <li>Policies and procedures are put in place by the administrator team that only administrators have the highest level of access and that role-based access controls restrict system access and sets permissions to only authorized users and their specific roles.</li> </ol> <p>Applicants:</p> <ol style="list-style-type: none"> <li>The applicants can only access and edit the PII they provide themselves, not any other applicants' PII.</li> <li>Applicants need system access to fill out and submit the application and track the approval progress of their application.</li> <li>Applicants can create their own user accounts and will be granted access based on a single portal user security role.</li> <li>Access can be manually changed or removed as necessary by administrators.</li> <li>Policies and procedures are put in place by the administrator team that only administrators have the highest level of access and that role-based access controls restrict system access and sets permissions to only authorized users and their specific roles.</li> </ol> <p>Application Reviewer/approval team:</p> <ol style="list-style-type: none"> <li>They can view and access all PII provided by the applicant.</li> <li>They need access to the applications to be able to view application information, review the applications for compliance and assess the applicant's ability to receive funding against predefined criteria. They will also be able to advance the application to the next step in the review process.</li> </ol>
--	--



	<p>c. AmeriCorps will review system access request. If approved, AmeriCorps will send the individual’s name, email address, and security role to Ernst &amp; Young for further action.</p> <p>d. AmeriCorps will notify Ernst &amp; Young when an individual no longer requires access to the system. In addition, Ernst &amp; Young will perform an annual review of user accounts and request AmeriCorps to review/update system user access.</p> <p>Grantee and Sponsor Portal audits the following activities: field-level changes, adding/removing users, changing roles, logon attempts, authentication checks, and permission changes. EY will complete audit record review, analysis, and reporting on a monthly basis, or more frequently in the event of an incident per NIST 800-53, Audit &amp; Accountability Control Family.</p>
--	--

11- PII SHARING	
<b>11-1</b>	<p><b>Separately describe each entity that receives PII from the system and:</b></p> <ol style="list-style-type: none"> <li>a. <b>What PII is shared.</b></li> <li>b. <b>Why PII is shared.</b></li> <li>c. <b>How the PII is shared (what means/medium).</b></li> <li>d. <b>The privacy controls to protect the PII while in transit.</b></li> <li>e. <b>The privacy controls to protect the PII once received.</b></li> <li>f. <b>Any agreements controlling that PII.</b></li> </ol> <p><b>If PII is not shared outside the system, write <u>Not Applicable</u>.</b></p>
	Not Applicable.

12- PRIVACY ACT REQUIREMENTS	
<b>12-1</b>	<p><b>If the system creates one or more systems of records under the Privacy Act of 1974:</b></p> <ol style="list-style-type: none"> <li>a. <b>Describe the retrieval that creates each system of records.</b></li> <li>b. <b>State which authorities authorize each system of records.</b></li> <li>c. <b>State which SORNs apply to each system of records.</b></li> </ol> <p><b>If the system does not create a system of records, write <u>Not Applicable</u>.</b></p>
	Not Applicable.

13- SAFEGUARDS	
<b>13-1</b>	<p><b>Describe the technical, physical, and administrative safeguards that protect the PII in the system.</b></p>
	The system collects names and business contact information from individuals working for organizations that apply for award, from AmeriCorps employees and contractors who administer the system, and from external reviewers who evaluate





	<p>the award application. The PII is used for setting up and managing these users' accounts in this system. The users' business contact information is used to administer the award processes. AmeriCorps only uses this information for legitimate business purposes. This Privacy Impact Assessment provides details about the business purpose and the uses of information in this system.</p> <p>AmeriCorps has issued series of internal policies regarding the protection of data privacy, confidential information, and the government properties. The system is categorized as a system of moderate level of risks; accordingly, a set of comprehensive administrative, technical and logical controls measures that are commensurate with this risk level are to be implemented to protect the information of the system. This includes, but are not limited to, incorporating effective contractual clauses about information security, privacy, record management, and breach reporting in the contract, requiring all the users of this system to receive regular cyber security and privacy training and other role-based training and sign Rules of Behaviors (ROB) before they can be authorized to access this system, and regularly assessing and monitoring all the controls measures following the guidance issued by National Institute of Standards and Technology.</p>
<b>13-2</b>	<b>Describe the technical, physical, and administrative measures that protect PII if the system is being retired.</b>
	Not Applicable.
<b>13-3</b>	<b>State if a system security plan and privacy plan is completed and the date of control verification.</b>
	A system security plan and privacy plan are currently in development, and have not been completed yet.

14- DATA ACCURACY, ACCESS, AMENDMENT, AND CONTROL	
<b>14-1</b>	<b>Describe the steps taken to ensure PII is sufficiently accurate, relevant, current, and complete.</b>
	The data in the application will be checked for completeness. Beyond basic field-level constraints, AmeriCorps staff does not validate if username, organization phone numbers, or organization email address are entered correctly. If information needs to be corrected, users will be able to make corrections.
<b>14-2</b>	<b>Describe how an individual could view, correct, update, or ask to amend their PII.</b>



	Grantee and Sponsor Portal users can log into their user accounts to make updates to their information as appropriate. They can view, correct, update, and amend their own information.
14-3	<b>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.</b>
	For individual users, AmeriCorps requires their name, organization affiliation, business email address, and business phone number to maintain their accounts and ensure that AmeriCorps staff reviewing applications and managing awards can contact organizations about their applications and awards as needed. Individual users can update their PII as needed.
14-4	<b>State if PII handling processes apply automation technology for decision making and describe the measures taken to eliminate risk to privacy interests.</b>
	Automation technology is not used for decision making.

15- DATA RETENTION AND DESTRUCTION	
15-1	<b>Identify the National Archives and Records Administration (NARA) provided retention schedule for the system and provide a summary of that schedule.</b>
	<p>AmeriCorps Grantee and Sponsor Portal follows the General Records Schedule (GRS) 1.2.</p> <p>Grant and cooperative agreement program management records. The disposition is temporary, and records will be destroyed 3 years after final action is taken on the file. Longer retention is authorized if required for business use. The disposition authority is DAA-GRS-2013-0008-0007.</p> <p>Grant and cooperative agreement case files records. The disposition is temporary, and records will be destroyed 10 years after final action is taken. Longer retention is authorized if required for business use. The disposition authority is DAA-GRS-2013-0008-0001 (also applicable to successful applications records).</p> <p>Unsuccessful applications records. The disposition is temporary, and records will be destroyed 3 years after final action is taken on file. The disposition authority is DAA-2013-0008-0006.</p> <p>All other copies [of applications] have a temporary disposition, and records will be destroyed when business use ceases. The Disposition authority is DAA-GRS-2013-0008-0002.</p>



	<p>Final grant and cooperative agreement products or deliverables records. The disposition is temporary, and records will be destroyed when business use case ceases. The disposition authority is DAA-GRS-2013-0008-0003.</p> <p>Part of the records of AmeriCorps Grantee and Sponsor Portal are covered by General Records Schedule (GRS) 1.1., the disposition authorities include:</p> <p>DAA-GRS-2016-0013-0001  DAA-GRS-2013-0003-0001  DAA-GRS-2013-0003-0002  DAA-GRS-2016-0001-0001  DAA-GRS-2013-0003-0011  DAA-GRS-2013-0003-0004  DAA-GRS-2013-0003-0012  DAA-GRS-2013-0003-0003  DAA-GRS-2016-0001-0003  DAA-GRS-2016-0001-0004  DAA-GRS-2016-0001-0005  DAA-GRS-2017-0005-0001  DAA-GRS-2018-0003-0001  DAA-GRS-2018-0003-0002</p>
<p><b>15-2</b></p>	<p><b>Identify the role and process to coordinate with the parties involved the record retention and disposition.</b></p> <p>Ernst &amp; Young Grant Accelerator Program Manager will coordinate with AmeriCorps Records Officer in accordance with the General Records Schedules.</p>

<p><b>16- SOCIAL SECURITY NUMBERS (SSNs)</b></p>	
<p><b>16-1</b></p>	<p><b>If the system collects truncated or full social security numbers (SSNs):</b></p> <ul style="list-style-type: none"> <li>a. Explain why the SSNs are required.</li> <li>b. Provide the legal authority for the usage of the SSNs.</li> <li>c. Describe any plans to reduce the number of SSNs.</li> </ul> <p><b>If the system does not collect any part of an SSN, write <u>Not Applicable</u>.</b></p> <p>Not Applicable.</p>

<p><b>17- WEBSITES</b></p>	
<p><b>17-1</b></p>	<p><b>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>.</b></p>



	<p>The AmeriCorps Grantee and Sponsor Portal has the link to <a href="https://www.americorps.gov/privacy">https://www.americorps.gov/privacy</a>. The main page also includes a banner warning: AmeriCorps actively monitors this system and software activity to maintain system security, availability, and to ensure appropriate and legitimate usage. Any individual who intentionally accesses a federal computer or system without authorization, and who alters, damages, makes unauthorized modifications to, or destroys information in any Federal interest computer, or exceeds authorized access, is in violation of the Computer Fraud and Abuse Act of 1986 (Public Law 99-474). Any evidence of possible violations of proper use or applicable laws found as a result of this monitoring may be turned over to Corporation Management and law enforcement. Any individual found to be in violation of the system proper use rules or law could be punished with loss of system access, fines, and imprisonment. By proceeding, you hereby acknowledge your agreement with these terms and the system's rules of behavior and consent to such monitoring and informational retrieval for law enforcement and other official purposes.</p>
--	--

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