AmeriCorps
Privacy Impact Assessment (PIA)

1- GENERAL SYSTEM INFORMATION		
1-1	**Name of the information system:**	Aprimo
1-2	**System Identifier (3 letter identifier):**	Aprimo
1-3	**Unique Investment Identifier (Exhibit 53):**	Aprimo
1-4	**Office or entity that owns the system:**	AmeriCorps Office of Information Technology (OIT)
1-5	**Office or entity that operates the system:**	Office of Communications and Marketing (OCM)
1-6	**State if the system is operational or provide the expected launch date:**	System is 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:**	The assessment for Aprimo is still ongoing with estimated completion date of mid-April.
1-9	**Approximate number of individuals with Personally Identifiable Information (PII) in the system:**	There are 32 AmeriCorps users currently have profiles in Aprimo system. In addition, the marketing material maintained in Aprimo might include photos and videos of some AmeriCorps members and volunteers and AmeriCorps webcasts.

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.**
	First 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>.**
	Not Applicable
4-3 A	**State whether this is the annual review of PIA.**
	Not Applicable
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.**
	Not Applicable
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)**
	Aprimo is a web-based software platform that provide content operations and marketing project management software solutions to manage content planning and creation. It integrates comprehensive marketing resources management capabilities with Digital Asset Management (DAM) functionalities that Aprimo offers as a Software as a Service (SaaS) solution to support digital rights management. The Aprimo platform that AmeriCorps procures facilitates secure brand portal on AmeriCorps' website, it directs users to the Aprimo service that AmeriCorps' Office of Communication and Marketing (OCM) employs to centrally store, organize, share, track and archive research and marketing materials that effectively serves AmeriCorps' network of over 2,000 grantees, sponsors, partners, staff, media and the public. Aprimo is FedRAMP certified.

AmeriCorps

6- INVENTORY OF PII	
6-1	**Provide a list of all the PII included in the system.**
	The members, volunteers or project sponsors/grantees of AmeriCorps programs might choose to voluntarily share their stories on AmeriCorps public websites, these stories might include their photos or videos. AmeriCorps also stores webcasts of its community service engagement events and speeches delivered by AmeriCorps senior leadership in Aprimo. Some of the videos are annotated with names, most often for leadership and occasionally the first name of an AmeriCorps member or volunteer. The names and email addresses of AmeriCorps users authorized to use Aprimo are maintained in the system for user account administration.

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 includes AmeriCorps staffs who are the users of Aprimo, AmeriCorps leadership and theses members and volunteers who voluntarily share their stories, photos and videos with AmeriCorps. The total numbers are less than 100.

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 digital asset management (DAM) functionality and capacity provided by Aprimo platform facilitates and maximizes AmeriCorps' utilization of various digital channels which significantly enhances AmeriCorps' program marketing capability and outreach. To appropriately provision and administer the user accounts, the essential credential information of AmeriCorps users is required and entered into the system by the system administrators. The name attached as an annotation of the webcast of AmeriCorps leadership maintained in Aprimo is part of the official work documentation of AmeriCorps and is only used for AmeriCorps official program management purpose. AmeriCorps only uses the photos and videos shared voluntarily by the AmeriCorps volunteers and members who have signed waiver and release of their exercise of covered privacy rights to AmeriCorps' use of those photos and video they share with AmeriCorps. These photos and videos are only used for promoting AmeriCorps' programs.

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
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
8-1 D	Describe any application of PII redaction, mask, anonymization or elimination.
	Not Application
8-1 E	Describe any design that is used to enhance privacy protection.
	All information within Aprimo is encrypted at rest using FIPS-Validated cryptography.

9- COLLECTIONS OF PII INTO THE SYSTEM	
9-1	Describe for each source of PII in the system: 1. The source. 2. What comes from that source. 3. How the PII enters the system.
	During the Aprimo account creation only staff emails and names are used. This information is entered directly by AmeriCorps staff. The photos and videos of AmeriCorps members and volunteers are shared directly by these individuals and centrally stored in AmeriCorps Aprimo. The webcasts of AmeriCorps are also maintained in Aprimo as part of the digital asset 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 **Not Applicable**.
	The photos and videos of AmeriCorps members and volunteers are only maintained and used by AmeriCorps after the member or volunteer signed waiver and release of their exercise of covered privacy rights to AmeriCorps' use of those photos and video they share with 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 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.**	

	Aprimo DAM tool will ensure that approved marketing and communications materials are readily accessible for AmeriCorps partners, including grantees and sponsors, to support their recruitment initiatives. OCM oversees the management of content within this tool. AmeriCorps's Aprimo users primarily fall into two groups which are Contributors and Administrators: 1. Contributors can upload digital assets such as photography, video, presentation, brochure, marketing Kits, presentations to the system and add taxonomy, as well as decide to whom those assets should be available. 2. Administrators, or contributors within the same user group can share drafts with another contributor. 3. Administrators can also upload digital assets to the system and do everything Contributors can do. Additionally, administrators can add users, adjust permissions and user groups, add or adjust taxonomy terms, and delete assets. Others (Consumer) can access Aprimo but can only view digital assets, they cannot edit digital assets or their taxonomy.	

Access to Aprimo is authorized on strict need-to-know basis in accordance with AmeriCorps cyber security policy and the Aprimo Information Classification Standard. Aprimo staff must be authenticated by and authorized via a centrally managed directory service prior to being granted access to the infrastructure components or code repositories through Aprimo networks. Management of the directory service are restricted to a limited number of privileged users which are authorized by IT Services and are responsible for the implementation of formal processes for user registration/deregistration. The Aprimo Customer Data Handling Policy ensures AmeriCorps data is handled responsibly. Aprimo facilitates AmeriCorps controlling authorization to AmeriCorps data.

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.

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>.**
	Not Applicable

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 Aprimo system is safeguarded through multiple layers of control to protect the information in the system. The information assets in Aprimo are classified into risk-based categories with compatible access controls. The administrator of Aprimo

		must sign an AmeriCorps Privileged User Rules of Behavior form and receive privacy and security training when onboarding and annually thereafter. Meanwhile, AmeriCorps requires all AmeriCorps employees and contractors go through annual security and privacy training, role-based privacy training, role-based breach response training and record management training to maintain adequate level of knowledge and awareness of data privacy and data security for performing their daily duties. Aprimo platform equips Americorps with state-of-the-art capability to centrally store, manage, and share its marketing material as digital assets via various digital channels. To ensure that AmeriCorps maintains and uses its marketing materials lawfully, AmeriCorps provides AmeriCorps members and volunteers or other individuals the opportunity to consider their choices and only accept photos and videos from these individuals after they sign waiver and release of exercising their ownership and privacy rights to what they share. To protect the information in Aprimo system appropriately, other privacy and data security measures and controls are also being implemented in Aprimo, commensurate with the requirements for a system with moderate system risk level. Per contract stipulation, the Aprimo provider is required to properly handle AmeriCorps record per the record retention schedule that are being identified by AmeriCorps.
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 (SSP) is completed in August of 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.**
		Not Applicable.
14-2		**Describe how an individual could view, correct, update, or ask to amend their PII.**
		Not Applicable.
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.**
		Not Applicable.

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 of Aprimo will be maintained permanently until its record retention schedule is approved by NARA.
15-1	Identify the role and process to coordinate with the parties involved the record retention and disposition.
	The Information System Owner will coordinate the record retention activities with the agency records officer. The records of Aprimo will be maintained permanently until its record retention schedule is approved by NARA.

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**.
	Not Applicable

18- OTHER PRIVACY RISKS

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