AmeriCorps
Privacy Impact Assessment (PIA)

1- GENERAL SYSTEM INFORMATION		
1-1	**Name of the information system:**	AmeriCorps Information Model (AIM)
1-2	**System Identifier (3 letter identifier):**	AIM
1-3	**Unique Investment Identifier (Exhibit 53):**	
1-4	**Office or entity that owns the system:**	Enterprise Data Management, Office of Chief Data Officer (CDO)
1-5	**Office or entity that operates the system:**	AmeriCorps Office of Information Technology (OIT)
1-6	**State if the system is operational or provide the expected launch date:**	System is not yet 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:**	ATO is in process.
1-9	**Approximate number of individuals with Personally Identifiable Information (PII) in the system:**	Currently, records of three million individuals flow from other systems and transactional databases into AIM for data governance processing. This number will increase over time.

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 the first PIA for this 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. This is the first PIA for this system.
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. This is the first PIA for this system.
4-3 C	**Describe objects and results of audit or tests (continuous monitoring).**
	Not Applicable. This is the first PIA for this system.
4-3 D	**Certify and state “Completion of Review” if no change occurs.**
	This is the first PIA for this system.
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).

Data is the core of AmeriCorps business. AmeriCorps uses 25 authorized internal systems and relies on nine external systems to maintain agency business operations. To establish governance for data generated by these systems, AmeriCorps CDO team develops the AmeriCorps Information Model (AIM) system which provides the logical structure and processes for maintaining AmeriCorps' trusted data. AIM provides the Data Hub and Trusted Data capabilities that are essential to AmeriCorps data modernization and will be tools for AmeriCorps CDO and data stewards to manage AmeriCorps Data with standardized Data Governance, Catalog, Data Storage, Master Data Management (MDM), Data Profiling, Quality & Transformation, Trusted Data Self-Service Business Analytics, Trusted Data Feedback Loop to Source Systems, and Data Sharing. AIM will substantially streamline AmeriCorps enterprise data management processes, enhance CDO's data analysis capability, improve the efficiency to address critical data issues, and establish and optimize AmeriCorps' data-driven decision-making processes.

AIM is comprised of five primary data processing tools that will make up the Enterprise Data Management infrastructure for AmeriCorps, which include Microsoft Purview, Profisee, Microsoft Azure Data Lake Storage Generation 2 (ADLS Gen2), Synapse Analytics, and Power BI.

- Microsoft Purview: Purview provides a unified data governance solution to help manage and govern AmeriCorps Data. AmeriCorps uses Purview AmeriCorps for following purposes:
    1) Maintain up-to-date map of all agency data sources.
    2) Automatically classify data elements, e.g., SSN, email.
    3) Manage access to data sources with Microsoft Entra ID.
    4) Enable data lineage,
    5) Utilize metamodels to add business metadata for context,
    6) Manage AmeriCorps Data Catalog, and Business Glossary,
    7) Provide content labeling.

- Profisee: AmeriCorps utilizes Profisee to master critical data domains, create master reference data, create a bidirectional integration with AmeriCorps data systems that allow for an integrity feedback loop.

- Microsoft Azure Data Lake Storage Generation 2 (ADLS Gen2): ADLS Gen2 provides robust, secure, and flexible data storage. In the AIM framework, the data lake decouples trusted data from the day-to-day transactional databases, allowing for efficient and independent data handling. The data lake ingests raw, unprocessed, structured, and unstructured data from AmeriCorps' diverse systems.

- Synapse Analytics: AmeriCorps utilizes Synapse Analytics to manage data profiling, quality, and transformations. Synapse Analytics is a SaaS Enterprise analytics service that provides a platform for data exploration, create pipelines for data integration and Extract, Transform, and Load (ETL)/ Extract, Load, and Transform (ELT), and integrate AmeriCorps multiple systems into ADLS Gen2.

- Power BI: AmeriCorps utilizes Power BI as self-service business analytics platform, to develop pre-defined dashboards for accessing AmeriCorps data and provide an option for Data Analysts outside of the CDO to pull and structure data reports.

6- INVENTORY OF PII

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

AIM's five primary data processing tools make up the Enterprise Data Management infrastructure for AmeriCorps. AIM is used to produce and maintains map of all agency data sources, classify data elements, enable data lineage and manage access to data sources, add business metadata for context, manage AmeriCorps data catalog and business glossary, and provide content labeling.

The CDO team utilizes AIM to establish governance for data generated by 25 internal systems approved for AmeriCorps day-to-day operations, and nine external systems AmeriCorps used for agency business operations. The data AIM handles might include PII collected and maintained by these internal and external systems. There may be systems that contain AmeriCorps data that the CDO elects not to bring to AIM.

The data lake of AIM might also store data generated as the results of information sharing with other federal agencies for the purpose of conducting statistical analysis of AmeriCorps members or volunteer service or alumni career pathway. The data maintained typically will include information used to uniquely identify an individual, such as name, SSN, and information related to the member or volunteer service credentials or career interests or pathway.

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.

		This AIM system is used to provide data governance and data management infrastructure services. The data it handles are essentially from other AmeriCorps systems that collect information from AmeriCorps staff, public individuals, AmeriCorps volunteers and members, and grantees' representatives. For more information about AmeriCorps systems that collect and maintain PII, please review the PIA published on AmeriCorps' privacy program website at www.AmeriCorps.gov/privacy.

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.**
	AIM system is used to provide data governance and data management infrastructure services. The data it handles are from other AmeriCorps systems. For more information about AmeriCorps systems that collect and maintain PII, please review the PIA published on AmeriCorps' privacy program website at www.AmeriCorps.gov/privacy. The data lake of AIM might also store data generated as the results of information sharing with other federal agencies, which typically will include PII collected by AmeriCorps systems that are used to uniquely identify an individual, and information related to the member or volunteer service credentials or career interests or pathway that other federal agencies share with AmeriCorps, permitted under relevant laws, regulations or Executive Orders, and are covered by federal government-wide system of records notices (SORNs) and AmeriCorps' SORNs.
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.**
	The system might store aggregated information shared by other federal agencies about individuals who provide member or volunteer service to AmeriCorps for the purpose of analyzing its program outreach and the impacts on the career pathway of the individuals who enrolled in AmeriCorps' member or volunteer services.
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.**
	AIM may pull in publicly available data (i.e. Census or congressional districting data) to support analytical functions required for reports and dashboards that are utilized in the agency. An example would be Congressional Data that is pulled from Melissa Data to support the build out of the agency's National Service Reports, that are published annually.
8-1 D	**Describe any application of PII redaction, mask, anonymization or elimination.**

	AIM implements specific segregation measure on PII data and non-PII data.
8-1 E	**Describe any design that is used to enhance privacy protection.**
	Access to data in the system is only granted to users who have the need to know by the system owner. There are specific roles defined and configured in the system, each role can only have access to data via an official approval and authorization process.

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.**
	AmeriCorps uses 25 authorized internal systems and relies on nine external systems to maintain agency business operations. To establish governance for data generated by these systems, AmeriCorps CDO team developed the AIM system which provides the logical structure and processes for maintaining AmeriCorps's trusted data. The data lake of AIM might be used to store information shared by other federal agencies about the career path of individuals who provide member or volunteer service in AmeriCorps' programs. This information is only used for statistical analysis.
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 data processed by AIM are from other systems of AmeriCorps, which might collect and maintain PII. AIM also store data obtained from other federal agencies via information sharing process. The PII collected by AmeriCorps or shared by other federal agencies are covered by either AmeriCorps' SORN or the SORN of other federal agencies. For more information about the privacy controls that AmeriCorps implemented for its specific systems, please review the PIA published on AmeriCorps website at https://www.AmeriCorps.gov/privacy. Information about the federal governmentwide SORN can also be accessed via the links provided on AmeriCorps' website https://www.AmeriCorps.gov/privacy.
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 Not Applicable.
	All the data processed by AIM are from other systems of AmeriCorps, which might collect and maintain PII. For more information about these systems, please review the PIA published on AmeriCorps website at . The data lake of AIM might store information shared by other federal agencies for programmatic statistical analysis only. These data sharing activities are covered by AmeriCorps' SORN and federal governmentwide SORN published publicly.
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 signs Memorandum with other federal agencies and goes through standard Information Sharing Privacy Evaluation process before it shares or obtain data from other federal agencies.

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.**
	Data processed by AIM are segregated into separate zones with different security protocols. The Raw-Data zone which might contain PII from other systems is subject to strict access control. The system administrators and user roles such as data curators who have the need to access the Raw-Data zone are required to submit an access request for approval and authorization before they can be granted minimal access to the data in this zone to do their assigned tasks. After the data in Raw-Data zone is processed and the data governance transformation processes are completed, the data will be maintained in another zone ready for AmeriCorps business users to use. Per AmeriCorps' system access control requirement, each role's level of access to the information handled by AIM system is tailored so as to be in compliance with

		the requirements of AmeriCorps privacy policy and cyber–security policy. These measures are subject to system level auditing process documented in the AIM System Security and Privacy Plan. The roles within the AIM system include System Admin and Curator Roles, and there will be users of the information (AmeriCorps Workforce) that will have access to the information in the form of reports and dashboards.

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. PII sharing agreements.** **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.**	
		AIM processes financial data from MAPR and transmit transactional data to ARC shared services via an SFTP connection to complete financial transactions. This financial data may include PII such as Employee Identification Number, Taxpayer Identification Number, Name and Personal Contact Information. Some external data requests will be centrally managed by CDO, and the data will be pulled through AIM. These data requests will be assessed via AmeriCorps' standardized Information Sharing Privacy Evaluation process before they can be approved. The evaluation covers the legal authority of the request made by external organizations, the specific data management and governance capabilities that AIM provides, the data security protection measures that must be in place for data at rest and in transit, and the terms of the data sharing agreement with external organization.

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 data processing environments and the technical, physical, and administrative safeguards (including vendors') that protect the PII in the system.**
	Data processed in AIM will be only in electronic form. AIM system inherits all the required auditing and Role Based Access Controls (RBAC), which include the ability to see which users have access to the data as well as which users have accessed the data. All data is encrypted in transit and at rest. Audit logs for all Azure resources for data lake are created automatically and will be reviewed quarterly or more often if necessary. In the event there is a breach, AIM will follow the AmeriCorps breach response policy and procedures. The AIM team will follow the standard Annual Security and Privacy Training for agency employees and contractors, which also includes Rules of Behavior (ROB) and confidentiality agreements/non-disclosure agreements where necessary. Access to the AIM system is granted to users on a need-to-know basis following documented procedures which specify which role(s) the user should be given, and which resource(s) they should have access to. These staff are also required to complete role-based privacy training before their access is authorized. Data is backed up automatically in Azure databases, as well as replicated using access geo-redundant storage. The data will be retained and disposed via identified record retention schedule. AIM has written supportive system documentation and Standard Operating Procedures (SOP) that provide specific instruction, procedural requirement and guidelines on master data management strategy and other relative data governance management and life cycle data management processes.
13-2	**Describe the technical, physical, and administrative measures that protect PII if the system is being retired.**
	Not Applicable. This is a new system.
13-3	**State if a system security plan and privacy plan is completed and the date of control verification.**
	System is in the process of getting an initial ATO and is about to go through the full assessment process. The system security plan and privacy plan are currently under development.

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.**
	AIM is used to provide data governance management to data of AmeriCorps systems. The source systems that handle PII are required to ensure the PII is accurate, relevant, current, and complete as part of the data privacy and data security protection assurance management process.

14-2	**Describe how an individual could view, correct, update, or ask to amend their PII.**	
		AIM is used to provide data governance management to data of AmeriCorps systems. An individual can contact AmeriCorps to have their PII in a system of records of AmeriCorps corrected, updated or amended by following the instruction provided by relevant System of Records Notice and PIA published on AmeriCorps website at https://www.AmeriCorps.gov/privacy.
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.**	
		AIM is used to provide data governance management to data already in AmeriCorps systems. The data lake of AIM might store information shared by other federal agencies for programmatic statistical analysis. These data sharing activities are covered by AmeriCorps' SORN and federal governmentwide SORN published publicly which provide details about the notice and consent processes and the rights that the individuals can exercise.
14-4	**State if PII handling processes apply automation technology for decision making and describe the measures taken to eliminate risk to privacy interests.**	
		AIM does not use automation technology.

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.**	
		AmeriCorps is currently in the process of updating, revising, and implementing the agency record retention schedule and internal assurance process policy. The records will be maintained indefinitely until a record retention schedule is identified and approved by the National Archives and Records Administration.
15-1	**Identify the role and process to coordinate with the parties involved the record retention and disposition.**	
		The System Owner and AmeriCorps records officer will coordinate record retention and disposition. The details of this process are under development. Once a schedule has been determined, records in AIM can either be automatically scheduled for deletion based upon that schedule or a more manual process could be put in place to delete the records according to a determined schedule.

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. AIM serves as a data governance tool. SSNs are collected by its source systems.

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.