



AmeriCorps Privacy Impact Assessment (PIA)

1- GENERAL SYSTEM INFORMATION		
1-1	Name of the information system:	AmeriCorps Financial Accounting and Integrated Management Information System (Momentum)
1-2	System Identifier (3 letter identifier):	MOM
1-3	Unique Investment Identifier (Exhibit 53):	485-000000010
1-4	Office or entity that owns the system:	CGI Federal Inc.
1-5	Office or entity that manages the system:	CGI Federal 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:	10/01/2022
1-9	Approximate number of individuals with PII in the system:	Momentum provides financial planning capabilities and means to record AmeriCorps' financial transactions and supports AmeriCorps' financial data exchange with other Federal agencies' systems. It processes approximately 1500 records weekly, the data it processes might contain PII as identified in other sections of this PIA. In addition, Momentum stores user information of approximately 200 AmeriCorps staff members who have access to the system.

250 E Street SW

Washington, D.C. 20525

202-606-5000/ 800-942-2677



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	<p>State whether this is the first PIA for the system or an update to a signed PIA.</p> <p>This is an update to a signed PIA.</p>
4-2	<p>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>.</p> <p>Momentum moved from a private cloud to a FedRAMP cloud in 2017. The Momentum application was upgraded from 7.0.2 to 7.5 in June of 2018. In October 2020, AmeriCorps started to utilize Oracle Financials of the Treasury Administrative Resource Center (ARC) through the Treasury Department’s Federal Shared Service. As the result of this transition, currently, only minimum functions of Momentum are maintained.</p>

5- SYSTEM PURPOSE	
5-1	<p>Describe the purpose of the system.</p> <p>To achieve AmeriCorps’ mission to improve lives, strengthen communities, and foster civic engagement through service and volunteering, AmeriCorps needs to maintain an environment for financial transaction integrity and internal controls which is fundamental to its core grant making function and assuring fiscal accountability to the public. To this end, AmeriCorps procures the follow-on licensing, software, and support services of proprietary Momentum® Software suite – Momentum, a multi-tier, distributed, Commercial off-the shelf (COTS) web-based enterprise financial management software system, from CGI Federal Inc (CGI).</p>



	<p>AmeriCorps Momentum (Momentum) provides financial planning capabilities and means to record AmeriCorps' financial transactions and supports AmeriCorps' financial data exchange with other Federal systems. Momentum records and integrates financial planning, purchasing, accounts receivable, accounts payable, payroll disbursements and other budget activities to ensure the currency and consistency of the transactions and related data. Momentum also provides AmeriCorps the functions needed to produce and provide financial reports used internally and externally to meet auditing and other compliance requirements.</p> <p>Momentum interfaces with several internal and external systems, including AmeriCorps's grants and member management system (eGrants/eSPAN/My AmeriCorps Portal), Department of Health and Human Services Payment Management System (PMS), and Department of Treasury. After the transition to using the Treasury Department's Federal Shared Service, only continued services for minimal functions including eGrants, eSPAN, PMS and Cost Share functionalities and related technical system support are still required from Momentum.</p> <p>Currently, CGI provides application hosting services (in CGI Federal Cloud), application license maintenance coverage, and professional services for the integration, on-going operations and maintenance (O&M) for AmeriCorps' implementation of Momentum suite of licensed product offerings.</p>
--	---

6- INVENTORY OF PII	
6-1	<p>Provide a list of all the PII included in the system.</p> <ul style="list-style-type: none"> • Individual Name • Social Security Number (SSN) when there is no alternative or Taxpayer Identification Number (TIN). SSN might be used as an Employer Identification Number if a business is a sole proprietorship and the owner chooses to use SSN as the EIN. Truncated SSN might be used to identify an employee. • Unique Entity ID (UEI) - a 12-character alphanumeric ID assigned to an entity by SAM.gov, which might be linkable to an individual registered to do business with the government. • Physical Address • Mailing Address • Payment Address



	<ul style="list-style-type: none"> • Bank Account Type • Bank Routing Number • Telephone Number • Email Address • Non-payroll Payment History
--	--

7- CATEGORIES OF INDIVIDUALS IN THE SYSTEM

7-1	<p>Describe the categories of individuals whose PII is in the system and state approximately how many individuals are in each category.</p>
	<p>In October 2020, AmeriCorps started to utilize Oracle Financials of ARC and only maintains minimum functions as aforementioned. The business processes remain in Momentum and interface to Oracle include processing cost share, member payroll and trust for eSPAN, and grants for eGrants and PMS. As a result, information such as Rule Publication Information, Budget Formulation Information, Debt Collection Information, User Fee Collection Information, Cost Accounting/ Performance Measurement Information, and Records Retention Information is now processed by ARC. Momentum only handles information relating to Budget Execution Information, Travel Information, Assets and Liability Management Information, Reporting and Information, Funds Control Information, Accounting Information, Payments Information, and Collections and Receivables Information.</p> <p>This information might contain PII of the categories of individuals to whom the grants payment will be made, who might owe money to AmeriCorps, or with whom AmeriCorps does business. Momentum maintains grant payment records, no PII is maintained by Momentum for the transaction handled for Trust and Member Payroll.</p>

8- INFORMATION IN THE SYSTEM

8-1	<p>For each category of individuals discussed above:</p> <ol style="list-style-type: none"> 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.
	<p>No individual's payment information is directly collected by Momentum.</p>



	<p>Momentum handles the information needed to ensure that AmeriCorps accurately records, processes, monitors, justifies, and reports all its financial transactions. Specifically, Momentum handles records or documents that might contain information as follows:</p> <ul style="list-style-type: none"> • Names, contact information, SSNs, and bank account information about any individual to whom that AmeriCorps intends to pay. AmeriCorps or the Department of Treasury might use this information to ask an individual certain question or to provide an individual with any document about a payment (e.g., receipt or check). The Department of Treasury might use the SSN and bank account information to send payment to an individual and report any taxable income to the Internal Revenue Service. • The name of any individual that owes or gives money to AmeriCorps (e.g., collections and donations), and information about the gift type, amount, employer matching, etc. • Business contact information (e.g., names, job titles, phone numbers) from individuals who represent an organization which AmeriCorps intends to make payment to or owes or gives money to AmeriCorps. AmeriCorps or the Department of Treasury might ask a question about the transaction and provide documents about the payment. • Documents needed to justify the purpose of each financial transaction. For example, a payment to a university for an education award may include the request from the service member and documents showing AmeriCorps' approval. AmeriCorps collects this information in case there are questions as to why a financial transaction occurred. • Any document related to a procurement including all proposals. This may include the contact information of company representatives and the resumes of people who may support that contract. AmeriCorps collects this information in case there are questions as to why a vendor was selected or the terms of that agreement.
--	--

9- COLLECTIONS OF PII INTO THE SYSTEM	
9-1	<p>Describe for each source of PII in the system:</p> <ol style="list-style-type: none"> The source. What comes from that source. How the PII enters the system. <p>Momentum handles the information needed to ensure that AmeriCorps accurately records, processes, monitors, justifies, and reports the financial transactions for VISTA Members, Trust, Cost Share, and Grants. Data in this system is obtained from (1) Documents submitted by individuals, and (2) documents issued by AmeriCorps officials involved with managing and disbursing funds.</p> <p>Specifically, when conducting transaction activities (i.e., commitment and obligation for eGrant, payroll and trust for eSPAN, prepayment, expenditure and</p>



	<p>receipt for PMS), Momentum may process and record the names, SSNs, and bank account information (e.g., account type, address, routing number, account number) of individuals that AmeriCorps intends to pay (VISTA Members, Peer Reviewers); and the names, Taxpayer Identification Number (TIN), and address of the grantee. Momentum may upload and process document that has PII. These documents are needed to justify the purpose of each financial transaction. For example, a payment to a university for an education award may include the request from the service member and documents showing AmeriCorps' approval. AmeriCorps collects this information in case there are questions as to why a financial transaction occurred</p> <p>Momentum collects the name and email address of AmeriCorps employees who are authorized to access Momentum to process transaction and manage the system.</p>
<p>9-2</p>	<p>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>.</p> <p>The data that Momentum handles are from documents submitted by individuals as well as documents issued by AmeriCorps officials involved with managing and disbursing funds. Further information is provided in the following section.</p>
<p>9-3</p>	<p>If PII about an individual comes from a source other than the individual, describe:</p> <ul style="list-style-type: none"> 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. <p>If all PII about an individual comes directly from the individual, write <u>Not Applicable</u>.</p> <p>There are information sharing with US Department of Treasury (including Collections Information Repository - CIR, the system managed by the Bureau of Fiscal Service and is used to show federal government transactions that have been cleared and deposited), Department of Health and Human Services (HHS), and Accuity. Weekly uploads of batch information containing total payments made, refunds, and cancellations are made from eSPAN database to Momentum. The Department of Health and Human Services (DHHS) Payment Management System exchanges information with Momentum, and this information is, in turn, provided back to the eSPAN database. Data from Accuity and CIR is exchanged with Momentum.</p> <p>Most PII in Momentum comes from other systems mentioned above that collect PII directly from individuals and employ appropriate safeguards to assure the collected PII is accurate (<i>See PIP PIA of the Department of Treasury and eSPAN PIA of AmeriCorps</i>). AmeriCorps and its Momentum vendor implemented additional safeguards to assure that PII is accurately transferred into Momentum as stipulated in the Interconnection Security Agreements (ISAs) and/or Memorandums of</p>



	<p>Understanding (MOUs). The response to Question 11-1 includes additional details about the PII that goes from other systems into Momentum.</p> <p>PII not collected from another system is either transcribed or uploaded by AmeriCorps staff. This PII often comes from documents used across the Federal Government and might be for one of the uses as authorized yet do not specifically mention Momentum. However, individuals who request or receive payment from AmeriCorps, offer or are asked to pay AmeriCorps or are included in an AmeriCorps proposal or contract are notified of the routine use of these information in these systems.</p>
9-4	<p>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>.</p>
	<p>Not Applicable</p>
9-5	<p>If any collections into the system are subject to an agreement, describe those agreements. If no agreements are relevant, write <u>Not Applicable</u>.</p>
	<p>Momentum will not collect PII from an external system until one or more agreements have been developed and signed to establish the appropriate controls. There is currently a:</p> <ul style="list-style-type: none"> • MOU and ISA governing PII received from the U.S. Department of the Treasury Bureau of the Fiscal Service Payment Application Modernization (PAM). • MOU and ISA governing PII received from The Electronic-System for Programs, Agreements and National Service Participants (eSPAN). • Memorandum of Agreement and ISA governing data exchange between CIR system and Invoice Processing Platform (IPP) system residing on Fiscal Service Treasury Web Application Infrastructure (TWA) and Momentum ISA and contract between AmeriCorps and CGI.

10- SYSTEM ACCESS

10-1	<p>Separately describe each category of individuals who can access the system along with:</p> <ol style="list-style-type: none"> 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.
	<p>About 200 AmeriCorps staff members have access to Momentum. About 100 have an AmeriCorps credit card, use Momentum solely to confirm their credit card statements are accurate, and only have access to PII about themselves. The other</p>



100 users may have access to PII about other individuals. Momentum has many user roles to assure they receive the least amount of PII necessary for their role. For example, a user whose role is limited to vendor payments will not receive access to PII about service members.

To obtain an account, (1) the requesting user must agree to abide by the AmeriCorps Rules of Behavior and (2) both their supervisor and system manager must confirm that the requested account type allows the minimum amount of access needed for their role. On a regular basis, both supervisors and system managers review all user accounts to confirm users still need that level of access. Anyone who leaves AmeriCorps and loses access to their AmeriCorps account also loses access to Momentum. An auditing system automatically notifies the system administrators if a change to a user's access rights is unusual.

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.

Momentum connects with the eSPAN- Electronic-System for Programs, Agreements and National Service Participants:

- eSPAN stores and manages PII about current and former AmeriCorps Members (Members). It includes details on when service members should receive their living expense, educational award, or certain types of payments. Weekly uploads of information containing total payments made, refunds, and cancellations are made from eSPAN database to Momentum. eSPAN sends the payment instructions to Momentum, which sends it to PAM for payment; PAM sends the payment confirmation to Momentum which forwards it to eSPAN. Momentum retains PII about all of these transactions.

Momentum shares PII with other external Federal systems:

- **U.S. Department of the Treasury Bureau of the Fiscal Service Payment Application Modernization (PAM):** eSPAN exchanges data with the U.S. Treasury, through Momentum, for payroll processing. eSPAN information is transferred to Treasury to provide payments to institutions. AmeriCorps uses PAM to distribute the Agency's funds. Each weekday, Momentum sends PAM an invoice file which states the amount to pay a recipient, their



	<p>banking information, and their contact information. PAM directs the bank to move the money to those accounts and then informs Momentum whether the payment was successful. If the payment fails, Treasury may use the contact information to resolve the problem. This process is used to pay living expenses, stipends, educational awards, and several other AmeriCorps expenditures.</p> <ul style="list-style-type: none"> • Accuity Bank: Momentum exchanges information with Accuity Bank by loading monthly bank file for accurate bank and routing data. • Collections Information Repository (CIR): Extract files are pulled from TWAI to be processed by Momentum. CIR transactions are for cost share receipts from ACH credit, Pay.gov and OTCnet. The cost share program is one of the programs of the AmeriCorps VISTA Office. The cost share program involves the sponsor agencies having to share in the cost of the project – to provide stipend to cost share members. <p>All of this PII is sent in encrypted form.</p>
--	---

12- PRIVACY ACT REQUIREMENTS

12-1	<p>If the system creates one or more systems of records under the Privacy Act of 1974:</p> <ol style="list-style-type: none"> Describe the retrieval that creates each system of records. State which authorities authorize each system of records. State which SORNs apply to each system of records. <p>If the system does not create a system of records, write <u>Not Applicable</u>.</p>
	<p>Momentum retrieves personal information about an individual using their name, or taxpayer identification number.</p> <p>The authorities for these systems of records are:</p> <ul style="list-style-type: none"> • Accounting Procedures Act of 1950, as amended • Budget and Accounting Procedures Act of 1950, as amended • Domestic Volunteer Service Act of 1973, as amended • Chief Financial Officer Act of 1990 • National and Community Service Act of 1990, as amended • National and Community Service Trust Act of 1993 • Debt Collection Improvement Act of 1996 • Executive Order 9397, as amended • 31 U.S. Code Subtitle III— Financial Management <p>AmeriCorps’ SORNs Corporation-1, Corporation-2, and Corporation-3 covers the PII handling activities of Momentum and the oracle financials that Momentum interfaces with.</p> <ul style="list-style-type: none"> • Corporation-1 - Momentum Financials Open Obligations and Automated Disbursement Files. This SORN applies to records of the payees.



	<ul style="list-style-type: none"> • Corporation-2 - Momentum Financials Accounts Receivable Files. This SORN applies to records of Individuals owing money to the Corporation. • Corporation-17 - Momentum Financials Vendor Files. This SORN applies to records of individuals with whom the Corporation does business.
--	---

13- SAFEGUARDS

13-1 Describe the technical, physical, and administrative safeguards that protect the PII in the system.

Momentum is designed to comply with applicable Federal security and privacy requirements.

Momentum has a documented process that details the structure of user accounts, how accounts are granted, and when they are disposed. All Momentum users receive the least amount of access required for their role. Account management procedures require the user’s supervisor to specify the access privileges to be granted based on the user’s job function. Procedures are in place to ensure that the concept of least privilege is applied when granting AmeriCorps Momentum Application accounts. System administrators and Database Administrators (DBAs) have access only to their designated OS platform, database instance, web server, VM management console, or other system components. All changes to an account go through an authorization process to confirm that the request is necessary; requests for privileged accounts require additional oversight. A process is in place to remove accounts when users no longer work for AmeriCorps or no longer require that level of access. Several controls including firewalls, an intrusion detection system, and auditing help assure that users do not access files they do not need.

User activity is closely audited and monitored, and unauthorized activity is referred to the appropriate official for action. Audits may include a time stamp, the type of event, the source IP and/or the username of the individual who made the change to the network.

All users must complete at least an introductory training before receiving access to PII in the system and a refresher training on an annual basis. The trainings explain the need for information security, how to maintain security, and how to respond to suspected security incidents.

All users must sign the AmeriCorps Cybersecurity User Rules of Behavior agreement confirming they understand applicable information security policies and procedures and will abide by them before they receive their account. All contractors with access to Momentum also must sign a nondisclosure agreement.

The users will see a warning banner when they attempt to access Momentum. The banner notifies the users that AmeriCorps monitors network activity and software usage to maintain system security, availability, and to ensure appropriate and



	<p>legitimate usage. It also states that users who intentionally accesses or damage information without authorization may be dismissed, fined and/or imprisoned.</p> <p>A strict configuration management program exists to approve and document all configuration changes made to system hardware or software.</p> <p>The PII in Momentum is maintained by the vendor in its off-site full-service data center. A limited number of staff have electronic access to the servers. Physical access is protected by safeguards which may include 24x7 security guards, close circuit cameras, and biometric security features.</p> <p>TLS, SFTP, and other techniques are used to encrypt sensitive data in transit. The only removable system media are system backup tapes, which are labeled appropriately and encrypted.</p> <p>Momentum undergoes an annual Security Assessment and Authorization (SA&A) by an independent third party.</p> <p>In the contract with the vendors, AmeriCorps clearly stipulates that AmeriCorps owns all the information handled by Momentum including all PII, that the vendor must comply with all the requirements to appropriately safeguard AmeriCorps' system and data. The vendor is required to notify AmeriCorps if there is an incident and have an incident response plan in place. On an annual basis, the plan is tested through a tabletop exercise and updated as needed. The record retention and disposition schedule of Momentum is identified. The records of Momentum are destroyed 6 years after final payment or cancellation in accordance with the NARA requirements. Longer retention is authorized if the records are needed for business use. AmeriCorps owns its data currently processed by ARC. Per the Inter Agency Agreement (IAA) between Americorp and the department of Treasury, ARC is responsible for the system and data security of Oracle Financial and ensures that the corresponding FISMA requirements are met.</p> <p>An audit log is created by Momentum per standard information security practice of AmeriCorps, which documents events, such as who modified specific set of PII, and times of event, etc.</p>
--	---

14- DATA ACCURACY, ACCESS, AMENDMENT, AND CONTROL	
14-1	<p>Describe the steps taken to ensure PII is sufficiently accurate, relevant, current, and complete.</p> <p>AmeriCorps and its vendor have implemented multiple safeguards to ensure that PII from other systems transferred into Momentum is accurate. These safeguards are documented in ISAs and MOUs which are reviewed on a regular basis.</p>



	<p>Steps are taken to assure PII in the source systems such as eSPAN is sufficiently accurate, relevant, current, and complete. The individuals can update their own PII via the source system or in the documents they submitted.</p> <p>AmeriCorps and its vendor also ensure that PII transcribed and uploaded by AmeriCorps staff is accurate, relevant, current, and complete by implementing measures listed below:</p> <ul style="list-style-type: none"> • There is a Momentum help desk where staff can email or call if they have questions on how to correctly use the system. • The software contains a basic online user guide and several AmeriCorps internal documents that further explain how to correctly use the system. • Staff transcribe PII into custom forms which are designed to collect the necessary details for each transaction. • The custom forms check whether the inputted data meets the expected format (e.g., phone numbers are 10 digits long). • Tasks in Momentum more susceptible to fraud (e.g., paying an invoice) are segregated, among two or more AmeriCorps staff members. For example, the staff member who enters an invoice into Momentum cannot approve payment of that invoice. • The documents that users upload into Momentum often include an image of the PII that is transcribed into Momentum. • Momentum creates an audit log which documents who modified specific set of PII.
<p>14-2</p>	<p>Describe how an individual could view, correct, update, or ask to amend their PII.</p> <p>Most PII in Momentum comes from other systems that may collect the PII directly from the individual (e.g., eSPAN and PAM). If PII in updated in those source systems, the same information in Momentum will be quickly updated.</p> <p>The published AmeriCorps SORNs covering the relevant system of records provide detailed information about how individuals can request access to or amend their record.</p>
<p>14-3</p>	<p>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.</p> <p>Momentum only maintains some financial records or handles information as aforementioned. These records might contain PII of the individuals who have established business relationship with AmeriCorps and have been notified of the routine uses of the PII collected from them. The PII is used only for the specific purposes for which the PII is initially collected by other systems. The individuals were provided options that allow them to either choose not to provide PII which is necessary for completing specific financial transaction which might result in their inability to receive or make payment, or consent with the PII collection.</p>



--	--

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 Record Retention Schedule for financial transactions and reporting is: General Record Schedule 1.1: Financial Management and Reporting Records, Item 10, DAA-GRS 2013-0003- 0001. The disposition is temporary. The records are destroyed 6 years after final payment or cancellation, but longer retention is authorized if required for business use.

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>.
	eSPAN and Oracle Financial of ARC uses SSNs to report taxable information of individuals to the IRS. Momentum does not collect SSN.

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