PRIVACY IMPACT ASSESSMENT	
Name of Information System or IT Project:	Momentum
Unique Investment Identifier (Exhibit 53):	485-000000010
System Identifier (3 letter identifier):	MoM
Date:(date the assessment was completed)	23 August 2011
Indicate whether this PIA is for a new system or for an existing system:	Existing system
Purpose of Information System or IT Project:(include if the system is a major application, minor application, or a general support system)	MoM is a major application and is the core financial system designed to provide and ensure accurate recording, processing, and reporting of financial transactions for the Corporation for National and Community Service.
Size of the Information System: (approximate number of users for the system)	200+ user
Security Categorization of the System: (e.g. Low, Moderate, High*)*	Moderate

CONTACT INFORMATION	
Person completing PIA: (Name, title, number, email.)	Nichole Vaughn Information System Security Manager (ISSM) 202-606-3903 NVaughn@cns.gov
Information System Owner: (Name, title, number, email.)	Adam Liu Information System Owner 202-606-6919 ALiu@cns.gov
Information System Security Manager (ISSM): (Name, title, number, email.)	Nichole Vaughn Information System Security Manager (ISSM) 202-606-3903 NVaughn@cns.gov

REVIEWERS	Signature	Date
Information System Owner Adam Liu	Original, signed copy on file with the CNCS OIT cybersecurity office.	7/8/2016
Office of General Counsel Alicia Wilson		
APPROVING OFFICIALS *(Contact CNCS by emailing privacy@cns.gov)*	Signature	Date
Chief Privacy Officer Amy Borgstrom		
Chief Information Security Officer Stacy Dawn		
Senior Agency Official for Privacy		

REVIEWERS	Signature	Date
Thomas R. Hanley, Jr.		

SYSTEM APPLICATION/GENERAL INFORMATION	
1. **Does this system contain any personally identifiable information (PII) about individuals?** (Any information collected, maintained, or used that is identifiable to the individual. If the answer is "No," mark the rest of this document as "N/A.")	YES
2. **Provide a link to where a list of all the PII data fields are documented within the system and also describe what PII will be collected or maintained by the system. If a link cannot be provided please provide the information in another form.** (e.g., First, Middle, Last Name; Social Security Number (SSN); Medical and Health Information; Financial Information; Clearance Information; Date of Birth (DOB); Employment Information; Work Address or Phone Number; Criminal History; Home Address or Phone Number)	Individual Name Social Security Number (SSN) or Taxpayer Identification Number (TIN) DUNS Number Physical Address Mailing Address Payment Address Bank Account Type Bank Routing Number Bank Account Number Telephone Number Email Address Non-payroll Payment History
3. **Is this system identified in the CNCS SORN?**	YES
4. **Are any modifications of the SORN needed currently?**	Yes, modifications are needed; updates are pending.

PII IN THE SYSTEM	
5. **What categories of individuals are covered in the system?** (e.g., public, employees, contractors, grantees, and/or volunteers. Members of the public refers to individuals in a non-employee or non-CNCS contractor context. Members of the public includes individuals for whom CNCS maintains information, as required by law, who were previously employed or contracted by CNCS. PIAs affecting members of the public are posted on the CNCS Privacy page of the public-facing website.)	CNCS Government Employees CNCS Government Contractors CNCS Present, retired officers, or employees Grantee Individuals CNCS Volunteers and Members

PII IN THE SYSTEM	
6. Why is the PII being collected?	Personally identifiable information must be collected in Momentum in order to ensure accurate recording, processing, and reporting of financial transactions for the Corporation for National and Community Service. The individual name and SSN/TIN, bank account numbers, and credit card numbers are collected so that disbursements can be made by Momentum through the Department of the Treasury to the individual and to report any taxable income to the Internal Revenue Service. The individual address is used to make payments by check and to report any taxable income to the individual, while banking information is used to make payments by electronic funds transfer. Telephone numbers and email addresses are collected for contact information in the event of a question on a financial transaction with the individual.
7. How will CNCS use the PII collected? (e.g., SSN are used to track education awards.)	Personally identifiable information collected and stored in Momentum is used to ensure the accuracy and supportability of financial transactions processed by CNCS. It is used to make payments; to establish and monitor accounts payable and receivable; to report taxable income to the recipient and to the Internal Revenue Service; and to fulfill financial management responsibilities of the Corporation for National and Community Service. Commercial data or publicly available data are not used in Momentum.
8. How will the PII be secured?	Any time personally identifiable information is transferred in or out of the hosting facility for Momentum the data is sent through a secure encrypted tunnel and web service endpoints. Transfers of data occur between the hosting facility and the National Finance Center for payroll information, Department of Treasury for payments, and CNCS headquarters for transfer to or from other CNCS systems (eSPAN and the Salary Management System). All users of CNCS computer systems undergo initial and periodic information security training and agree to abide by the Corporation Information Security policies. All CNCS staff participate in security and privacy training when their onboard and annually thereafter. They sign the CNCS Security and Privacy Rules of Behavior agreement prior to gaining access to the CNCS network and must resign as part of the annual security training. Users with Momentum access must also agree to the Momentum Rules of Behavior when they log in to the application.

PII IN THE SYSTEM	
9. **Is information being obtained from the individual directly? If not directly, then what are the other sources?**	Yes. Information may be collected directly from the individual in several ways. The individual may provide the information in person, electronically to CNCS staff, interfaced from an internal/external system/source, or by the use of a Standard Form 1199 Direct Deposit Authorization. Individuals may also provide certain data on a Travel Authorization request form.
10. **Is the PII current?** (What steps are being taken to ensure the PII is current and that there is not any PII that needs to be deleted? For example, if someone is no longer an employee, their PII is not needed after a certain point.)	Yes, the PII information is current, however, this is based on the latest information that was provided to CNCS from the individual(s) and organization(s). MoM System Administrations are the only Individuals that can update PII information via Momentum system, per the request of the individual. CNCS follows NARA's records retention schedule identified in question 15 to ensure that PII that is not needed is deleted.
11. **What specific authorities authorize this system or project, the associated collection, use, and/or retention of personal information?** (A Federal law, Executive Order of the President or CNCS requirement must authorize the collection. i.e., legal authority to collect SSN.)	Personally Identifiable Information is collected under the provisions of 31 USC 3511 (Accounting Requirements, Systems and Information) and 44 USC 3101 (Records Management). The National and Community Service Act of 1990, as amended (Pub. L. No. 101-610, as amended); the Domestic Volunteer Service Act of 1973, as amended (Pub. L. No. 93-113, as amended).
12. **What opportunities do individuals have to decline collection of specific PII/ consent to particular use and/or approve or disapprove of how that information is being shared?**	While an individual may decline to provide PII, in order to receive payment the personally identifiable information must be provided. Failure to provide the information could result in denial of the original action that would ultimately result in a payment (such as a travel order, purchase order or contract). Individuals do not have the opportunity to consent to particular authorized uses of the information provided.
13. **Are the PII elements described in detail and documented? If so, what document provides description?** (e.g., Data Management Plan)	PII elements are described in the SSP. All personally identifiable information is collected as a result of an action initiated by the individual. These actions include Travel Authorizations, Direct Deposit Authorizations (SF-1199), or individual response to accounting and/or procurement actions. Notice of the information collection prior to obligation is consistent with the ability of the Corporation to make payment for its liabilities.
14. **If the information system is operated at more than one site, how will consistency of the information be ensured at all sites?**	Momentum is operating at one site. Momentum is hosted at a data center under contract with the Corporation. The contract specifies that appropriate security measures be applied for all data handling and storage to include personally identifiable information.

MAINTENANCE AND ADMINISTRATIVE CONTROLS	
15. What are the retention periods of PII in this system? (This should be consistent with the records schedule as approved by the National Archives and Records Administration.)	Under the NARA General Records Schedule 1.1 item 010, CNCS retains records for at least 6 years and longer if it is determined that they are needed for administrative, legal, audit, or other operational purposes.
16. What are the procedures for disposition of the PII at the end of the retention period?	CGI employs sanitization mechanisms in accordance with NIST 800-88, Guidelines for Media Sanitization. The media is sanitized before use so that any information is properly destroyed by overwriting or degaussing. In addition, CGI has in place the Information Handling Standard that includes sanitization and disposal. The CGI IaaS Cloud Hitachi SAN provides a tool to sanitize the storage areas used by a customer once the customer releases the storage space on the SAN. CGI sanitizes the storage space on the SAN in accordance with DOD standards (DoD5220.22-M). As stated in MA-2, hardware maintenance occurs onsite at the data centers, and maintenance off premises is not permitted."
17. Does the system generate audit records containing information that establishes the identity of the individual associated with accessing the system's PII for accountability purposes (e.g., implemented audit logging)? If yes, what information is captured regarding users/usage?	Audit logging is enabled in Momentum on both the application and infrastructure level. Application actions including login, logout, and transactions applied are logged. Transaction logging in Momentum records user ID and timestamp support accountability for all changes recorded in the application. Infrastructure components such as databases and operating systems are also configured to log actions performed such as login, logout, privilege use, privilege escalation, and failed login attempts. Firewalls at the Momentum hosting facility will only allow authorized IP addresses to access the Momentum servers. Network activity logs track access attempts to the Momentum servers, and Momentum application logs track user actions and processed transactions. Full details of the security safeguards in place for Momentum are documented in the CNCS Momentum System Security Plan. Details regarding auditing capabilities, including the contents of audit trails, infrastructure and application auditing settings, and retention periods are also documented in the Momentum SSP.
18. Will the PII be retrieved using a personal identifier? List the identifiers that will be used to retrieve information and/or create reports.	Name and SSN can be used to retrieve a vendor record.

MAINTENANCE AND ADMINISTRATIVE CONTROLS	
19. What controls will be used to prevent unauthorized monitoring or retrieval of PII?	Momentum users must complete security background/ROB and request a userID in order to use the system. By applying for a Momentum account users agree to abide by the Momentum Rules of Behavior. Supervisors review and approves staff access and role requests based upon duties and need-to know. Senior System Accountant reviews the access request to ensure the user is granted the minimum privileges necessary to perform their duties. Momentum has many roles defined by CNCS' business processes, organizational structure, and program needs. Each role can be requested to provide needed access to the system, in accordance with principles of least privilege and minimum necessary access. Supervisors review individual access permissions quarterly to ensure that the permissions are still appropriate to the individual's duties.

ACCESS TO PII	
20. **Who will have access to the PII in the system? What kind of access will they have?** (e.g., contractors, managers, system administrators, developers, or others. Read only access, read and write access, or change. If contractors have access to the PII in the system, provide evidence that assigned contractors are in compliance with CNSC rules on privacy.)	Helpdesk contractors – access view limited PII data, limited to read-only, and cannot process documents, CNCS managers/employees - only on a need-to- know basis - access view data, change, and process documents in Momentum, Momentum System Administrators – access view all PII data, update reference tables, and cannot process documents. Momentum users must request a user ID in order to use the system. By applying for a Momentum account users agree to abide by the Momentum Rules of Behavior. Supervisors and Senior System Accountants perform periodic security reviews of each Momentum user. The Momentum user will have the approved access to data related to their business processes, organizational structure, and program needs. The general user will not be able to access any PII outside of their information. Contractors will have limited access to Momentum. Their authorized roles will normally be limited to read-only in the production environment. Contractors for the Momentum host may have the ability to execute predefined batch processes in production. All contractors must have a CNCS employee review their access request initially as well as on a quarterly basis as part of the overall Corporation access review policy.
21. **What controls are in place to prevent the misuse of PII by those having access and who is responsible for assuring proper use of the PII?** (Please list processes and training materials.)	The supervisor reviews the request and verifies the users need-to-know prior to requesting the necessary roles within Momentum. Senior System Accountant review the access request to ensure the user is granted the minimum privileges necessary to perform their duties. Senior System Accountant performs random ad-hoc security review throughout the year. The Senior System Accountant provides the supervisors a security role table guideline that describes the type of access for each role, as it relates to the security reviews. The quarterly security reviews are completed by supervisors for each Momentum user. Momentum has many roles defined by business processes, organizational structure, and program needs. Each role can be requested to provide needed access to the system, in accordance with principles of least privilege and minimum necessary access.

ACCESS TO PII	
22. Who will the PII be shared with? List other systems that share or have access to the PII. If other systems have access to or share the PII, is there an interconnection agreement in place or written agreement regarding the sharing and how the PII will be protected? How will the PII be used by the other agency and who will be responsible for protecting the privacy rights of the public and employees affected by any interface?	Data sharing of personally identifiable information (PII) outside of the Corporation is done in a manner consistent with the intent of the original collection of the information. PII is shared outside the Corporation only in ways that support the Corporation's mission and which are necessary for the accurate and continuing operation of the Momentum financial system. The below agencies are the only outside entities CNCS shares PII with. The Corporation has a Memorandum of Understanding with the Department of Treasury to disburse payment files and to report the results back to the Corporation. The Corporation has an Inter-agency agreement with the Department of Agriculture, National Finance Center to provide payroll services for the Corporation. The Corporation has an Inter-agency agreement with the Department of Health and Human Services to provide grant payment services for the Corporation. External file transmissions are with Federal agencies that are required to abide by the Privacy Act of 1974 as amended. Agencies are required to take appropriate action to protect personally identifiable information.
23. Will the information be saved to removable media, or printed to hard copy? How will removable media and or hard copies be protected?	Momentum is hosted at a data center under contract with the Corporation. The contract specifies that appropriate security measures be applied for all data handling and storage to include personally identifiable information. The following Media Protection controls are available for the CNCS Momentum Application: Removable media is protected from unauthorized internal users reading, copying, altering, or removing electronic information by using the role-based access control provided by the application. The only removable system media are the system backup tapes, which are labeled appropriately according to organizational procedures and are encrypted with AES 256-bit encryption. As no other removable media is utilized, there are no exemptions. The CGI Phoenix Data Center (PDC) does not allow use of any portable media device (USB key etc.) within the server area unless prior approval and authorization has seen granted. The use of personally owned removable media is forbidden by the PDC Data Center Security Policies. The only removable media utilized are backup tapes, which always have an identifiable owner.