PRIVACY IMPACT ASSESSMENT	
Name of Information System or IT Project:	eSPAN
Unique Investment Identifier (Exhibit 53):	485-000000004
System Identifier (3 letter identifier):	ESP
Date:(date the assessment was completed)	6/2/2016
Indicate whether this PIA is for a new system or for an existing system:	Existing
Purpose of Information System or IT Project:(include if the system is a major application, minor application, or a general support system)	The Corporation for National and Community Service (CNCS) relies on its information technology (IT) systems to accomplish its mission of cost effectively providing and managing volunteer services on a national basis. eSPAN (Electronic System for Programs, Agreements & National service participants) is the central database for maintaining Corporation application and grant data and AmeriCorps program and member data, including member related payment data. The eGrants component manages the Corporation-wide grant process from application creation to grant closeout. On average, the Corporation receives approximately 7000 applications and manages 2700 active grants each year. There are 5700 grantee and prospective grantee organizations with accounts in eGrants.- The Trust component manages the National Service Trust Fund which makes payments on behalf of members, and maintains membership and institution data. The Member Portal component provides program management and member data entry capability to program staff. The Member Portal is a self-service, on-line consolidation of information and processes specific to the AmeriCorps member experience and to member management. The Member Portal provides a system of processes for member support including recruitment, enrollment, service, close of service, and post-service. In addition, the Member Portal provides CNCS and Project Sponsors with a consistent interface for gathering necessary data from and about Members and Applicants. Trust Automation functionality will be incorporated into the Member Portal "platform".
Size of the Information System: (approximate number of users for the system)	20,351 eGrant users, 1,120,076 Member Portal users, 249 Staff Portal users, and 212 eSPAN users.
Security Categorization of the System: (e.g. Low, Moderate, High*)*	Moderate

CONTACT INFORMATION	
Person completing PIA: (Name, title, number, email.)	Donald McComas, PM, 202-730-2970, dmccomas@cns.gov Erick McKinley, ISSO, 703-730-2976, emckinley@cns.gov
Information System Owner: (Name, title, number, email.)	William Schmitt, System Owner, wschmitt@cns.gov, 202-606-6891
Information System Security Manager (ISSM): (Name, title, number, email.)	George Roehm, ISSM, 202-606-6778, groehm@cns.gov

REVIEWERS	Signature	Date
Information System Owner William Schmitt	**Original, signed copy on file with the CNCS OIT cybersecurity office.**	6/7/2016
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 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)	PII collected and maintained by eGrants for Peer Reviewers includes: • Social Security Number • Name • Private Address • Email address • Phone number • Bank account number PII collected and maintained by eGrants for Grantee organizations and CNCS staff includes: • Name of individuals within a Grantee organization • CNCS staff names

SYSTEM APPLICATION/GENERAL INFORMATION	
	PII collected and maintained by the Trust/eSPAN, Member Portal includes: • Name • Date Of Birth • SSN • Private Address • Demographics • Program service information • Lender and Educational Institution Data • Member education award • Financial Transactions Data.
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.)	Peer Reviewers, Members (volunteers through CNCS programs), former Members, and CNCS staff personnel.

PII IN THE SYSTEM	
6. Why is the PII being collected?	PII is collected in eSPAN in order to ensure accurate recording, processing and reporting of data, including financial transactions, for the Corporation for National and Community Service. Names and social security numbers are collected to verify eligibility for the program and so that disbursements can be made through the Department of the Treasury to institutions and to report any taxable income to the Internal Revenue Service. Personal and institutional addresses are used to make payments by check and to report any taxable income to the individual or to otherwise correspond with them. 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 or other transaction with the individual or institution. Also, this information is used to respond to questions and requests for statistical reporting. PII is also collected to manage project information and cost share billing, to compute member stipends, provide living allowances, childcare allowances, healthcare benefits, establish administrative holds, and process re-enrollments, extensions, early terminations, project transfers, reinstatements into the program, and completion of service for authorized members.
7. How will CNCS use the PII collected? (e.g., SSN are used to track education awards.)	CNCS will use the PII collected to ensure accurate recording, processing and reporting of data, including financial transactions, for the Corporation for National and Community Service. Names and social security numbers are collected so that disbursements can be made through the Department of the Treasury to institutions and to report any taxable income to the Internal Revenue Service. Personal and institutional addresses are used to make payments by check and to report any taxable income to the individual or to otherwise correspond with them. Banking information is used to make payments by electronic funds transfer. Telephone numbers and email addresses are used for contact information in the event of a question on a financial or other transaction with the individual or institution. Also, this information is used to respond to questions and requests for statistical reporting. PII is also collected to manage project information and cost share billing, to compute member stipends, provide living allowances, childcare allowances, healthcare benefits, establish administrative holds, and process re-enrollments, extensions, early terminations, project transfers, reinstatements into the program, and completion of service for authorized members.

PII IN THE SYSTEM	
8. How will the PII be secured?	CNCS limits the amount of personally identifiable information in eSPAN to the minimum necessary to support its customer and organizations. Controls are in place in the form of administrative policies and procedures, as well as technical controls, which ensure information is used in accordance with the above described uses. Access to personal information is limited to system users who have been approved and assigned a system role authorizing access to information required to perform their job functions. The ability to perform data mining, query directly against the database, or create data reports other than those authorized for their user role is controlled through access controls on the system. User's that are granted access to the eSPAN have signed a CNCS Cybersecurity Rules of Behavior Agreement that outline the roles and responsibilities while accessing a government system and consequences of misbehavior are also defined. Additionally, a standard CNCS warning banner is displayed on the eSPAN homepage to inform users that they are about to access a CNCS owned computer system: **The Corporation for National and Community Service monitors Network activity and software usage to maintain system security, availability, and to ensure appropriate and legitimate usage. Any individual who intentionally accesses a Federal computer 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 individual found to be in violation of this Act could be punished with fines and imprisonment, and/or dismissal. By proceeding, you hereby acknowledge your agreement with these terms.** CNCS also uses the following warning: *This Computer is U.S. Government Property* All access to the system is encrypted using TLS and controlled by users accounts and passwords.

PII IN THE SYSTEM	
9. **Is information being obtained from the individual directly? If not directly, then what are the other sources?**	Yes. Information is collected directly from the individual in several ways. Grant applicants, awardees, and Peer Reviewers enter information directly into the eGrants portal. AmeriCorps members and organizations enter their information electronically to CNCS using the MyAmeriCorps portal. AmeriCorps members, grantee organizations, and Peer Reviewers may, on occasion, provide information directly to the National Service Hotline
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.)	Member Information is provided directly by the individual and is self-certified. At any time, Members can log in to the Member Portal and update their information, and they are instructed to keep data current. Peer Reviewer information is provided directly by the individual and is self-certified and can be adjusted at any time thru the eGrants Portal. Grantee's information is provided at the time the application is submitted. The eGrants and the Member portals contain field level edit checks of the data input by applicants and AmeriCorps members for reasonableness at time of entry.
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.)	The primary statutes that authorize this collection of information are the Domestic Volunteer Service Act of 1973, as amended; the National and Community Service Act of 1990, as amended; Accounting Procedures Act of 1950, as amended; the Chief Financial Officer Act of 1990; and the Debt Collection Improvement Act of 1996.
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?**	Individuals can decline to provide information. However, in order to become a member or grantee, receive payment or other benefits or to process a member application, the personally identifiable information must be provided.
13. **Are the PII elements described in detail and documented? If so, what document provides description?** (e.g., Data Management Plan)	Yes. eSPAN System Security Plan.
14. **If the information system is operated at more than one site, how will consistency of the information be ensured at all sites?**	There is a separate Disaster Recovery/ Continuity of Operations Plan site which contains a replica of the main eSPAN application/database. We ensure consistency via our replication process. We also have a data warehouse which is also replicated in real time and verified by our replication tools and technology. Finally we are in the process of rolling out the new system GMM in which the eGrants data will be migrated and verified as part of rollout. It'll also be replicated using a tool called Mulesoft and verified accordingly using logs, testing and validation.

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.)	Programmatic data, including demographic and personal information, is maintained for historical purposes and assessing program trends and making forecasts. The records are maintained within the system indefinitely. Retention of financial data is similarly determined by federal accounting standards. Records that are forwarded to the archives for storage meet NARA requirements. With the eSPAN being phased out over the next two years retention of records will be managed by the Grants Member Management (GMM) system once in production and will conform to the CNCS record schedule.
16. What are the procedures for disposition of the PII at the end of the retention period?	All data is maintain indefinitely. With the eSPAN being phased out over the next two years retention of records will be managed by the Grants Member Management (GMM) system once in production and will conform to the CNCS record schedule.
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?	Network activity logs track access attempts to the eSPAN servers and the mod-user and date of significant events. eSPAN maintains a log for all processed transactions. eSPAN runs on the Oracle database that tracks activity within the Oracle Audit tables. Audit events Include login/login, changes made to records, who created records, and the dates associated with these events
18. Will the PII be retrieved using a personal identifier? List the identifiers that will be used to retrieve information and/or create reports.	Records can be retrieved using name, SSN, address, and date of birth.
19. What controls will be used to prevent unauthorized monitoring or retrieval of PII?	CNCS staff access is restricted by eSPAN roles and authorized CNCS staff has access appropriate to their assigned duties. Access must be approved by staff members' supervisor and the eSPAN data owner. Staff access is reviewed quarterly and adjusted as required. Members, institutions, and grantees have access to their own data and are given roles appropriate to their program requirements.

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 CNCS rules on privacy.)	Authorized CNCS staff (federal and contractor employees) have access appropriate to their assigned duties. Those individuals have limited access based on their roles within the system. Roles are assigned based on their supervisor's and business owner's approval and all individual roles are reviewed quarterly by their supervisor. CNCS contractors must follow the same process as federal employees to obtain access to the system. They also must follow the same Rules of Behavior and attend the same cybersecurity and privacy training as federal staff. Members, institutions, peer reviewers, and grantees have access to their own data in the system.

ACCESS TO PII	
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.)	CNCS staff must request access in order to use the system which is approved by both the supervisor and data owner. CNCS eSPAN accounts are reviewed quarterly and adjusted accordingly. Also, all CNCS staff receive annual security and privacy training and must sign the CNCS cybersecurity Rules of Behavior (ROBs). The training and ROBs contain instructions about the proper handling of PII and why it must be protected.
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?	eSPAN exchanges data with the U.S. Treasury, through Momentum, for member payroll processing and to provide payments to institutions. There is no direct connection between eSPAN and the U.S. Treasury's financial management system. An Interconnection Service Agreement (ISA) is in place between CNCS and CGI who owns the Momentum system. CGI maintains a ISA and MOU with the U.S. Treasury. PII is also shared with Social Security Administration to verify SSNs and provide citizenship status. This process is covered by computer matching agreement (CMA) and is reviewed annually.
23. Will the information be saved to removable media, or printed to hard copy? How will removable media and or hard copies be protected?	Data on tape is AES-128 encrypted and sent off site for secure storage with First Federal.