PRIVACY IMPACT ASSESSMENT	
Name of Information System or IT Project:	CNCS General Support System
Unique Investment Identifier (Exhibit 53):	485-000000014
System Identifier (3 letter identifier):	GSS
Date:(date the assessment was completed)	6/6/2016
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)	The CNCS General Support System (GSS) provides general automated data processing and support for CNCS and the general public using Corporation IT resources. Network services include security support as well as Mobile Device Management and Voice Over Internet Protocol (VOIP) telephone service. The Corporation GSS hosts or provides connectivity for Major Applications (MAs) such as the Electronic System for Programs Agreements and National Service Participants (E-SPAN), and the Momentum Financial Management System (Momentum). It also supports Minor Applications such as office automation, human relations, travel, and Freedom of Information Act (FOIA) and Privacy Act requests.
Size of the Information System: (approximate number of users for the system)	900
Security Categorization of the System: (e.g. Low, Moderate, High*)*	Moderate

CONTACT INFORMATION	
Person completing PIA: (Name, title, number, email.)	Lee Defibaugh, ISSO, 314-308-6840, lee.defibaugh@csra.com
Information System Owner: (Name, title, number, email.)	Pamela Leith, Infrastructure Manager, 202-606-6917, pleith@cns.gov
Information System Security Manager (ISSM): (Name, title, number, email.)	N/A

REVIEWERS	Signature	Date
Information System Owner Pamela Leith	Original, signed copy on file with the CNCS OIT cybersecurity office.	6/14/2016
Office of General Counsel Alicia Wilson		
APPROVING OFFICIALS *(Contact CNCS by emailing privacy@cns.gov)*	Signature	Date

REVIEWERS	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, the CNCS GSS stores a limited amount of PII which CNCS staff may manual download/save limited PII from other systems such as eSPAN, Momentum, GMM, and the childcare and health benefits system for specific business purposes. The PII from these systems is documented in each system's respective, governing System of Records Notice (SORN) and PIA[i].
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)	The GSS does not collect PII. CNCS offices may store on the GSS PII that is obtained from other sources. As there is no single system that is the source for various PII that is stored on the GSS, the following is a sample of the PII collected by CNCS' major applications (eSPAN, GMM, Momentum, and the childcare and health benefits systems) : • First Name • Last Name • Middle Initial • Date of Birth • Gender • Address (including e-mail) • All Phone Number Types • Social Security Numbers A complete list of PII from these other systems is documented in each system's respective, governing System of Records Notice (SORN) and PIA.
3. **Is this system identified in the CNCS SORN?**	No
4. **Are any modifications of the SORN needed currently?**	No. The GSS does not collect PII, nor is the information retrievable by any specific identifier. CNCS offices may store on the GSS PII that is obtained from other sources.

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.)	As there is no single system that is the source for various PII that is stored on the GSS, the category of individuals from the PII collected by CNCS' major applications (eSpan, GMM, Momentum, and the childcare and health benefits systems) include CNCS employees, members/volunteers, peer reviewers and individuals within a grantee organization. The category of individuals for each of these systems is in accordance with each system's respective, governing System of Records Notice (SORN) and PIA.
6. **Why is the PII being collected?**	The GSS does not collect PII. As there is no single system that is the source for various PII that is stored on the GSS, the reason PII is collected will be in accordance with each system's respective, governing System of Records Notice (SORN) and PIA.
7. **How will CNCS use the PII collected?** (e.g., SSN are used to track education awards.)	The GSS does not collect PII. As there is no single system that is the source for various PII that is stored on the GSS, how PII will be used will be in accordance with each system's respective, governing System of Records Notice (SORN) and PIA.

PII IN THE SYSTEM	
8. How will the PII be secured?	Controls and safeguards are evaluated on a continual basis. Risk assessments are performed and the Network GSS undergoes annual auditing. Changes are managed through a rigorous change management process which includes the determination if internal or external change notifications and related communications are needed. CNCS employs a suite of tools and systems to detect, remove, and block malicious code and to minimize the risk of network and user exposure. CNCS implements a defense-in-depth strategy in the Network GSS and participates in the federal government's continuous monitoring initiative. Access to information is based on the least privilege security model in which authorized administrators and users are given the smallest amount of system and data access that is necessary to accomplish their authorized tasks. Each new network user receives the most restrictive set of privileges and network access, and additional privileges and access must be authorized when appropriate. All network activity is closely audited and monitored, and unauthorized activity is referred to the appropriate official for action. Physical access to the Network GSS is controlled, logged, and monitored. CNCS has deployed a strict configuration management program to approve and document all configuration changes made to Network GSS hardware, software, and other components. CNCS policy states that electronic documents (including emails) containing Sensitive PII may be stored only on individually assigned CNCS network storage space or on a shared CNCS network drive in a file folder to which access has been restricted to authorized individuals. No personally owned devices are allowed to be connected to any IT asset within the Network GSS. Electronic documents (including emails) containing Sensitive PII must be transmitted using CNCS' approved secure file transmission solution.
9. Is information being obtained from the individual directly? If not directly, then what are the other sources?	As there is no single system that is the source for various PII that is stored on the GSS, the original method of data collection will be in accordance with each system's respective, governing System of Records Notice (SORN) and PIA.
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.)	As there is no single system that is the source for various PII that is stored on the GSS, the steps taken to ensure PII is current will be in accordance with each system's respective, governing System of Records Notice (SORN) and PIA.

PII IN THE SYSTEM	
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 GSS is collection of services and tools which enables the agency to conduct business and provide services identified in the Domestic and Volunteer Service Act of 1973, as amended (Pub. L. No. 93-113, as amended) and the National Community Service Act of 1990, as amended (Pub. L. No. 101-610, 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?	The GSS does not collect PII. As there is no single system that is the source for various PII that is stored on the GSS, the opportunities to decline PII is described in each system's respective, governing System of Records Notice (SORN) and PIA.
13. Are the PII elements described in detail and documented? If so, what document provides description? (e.g., Data Management Plan)	No. The GSS does not collect PII. As there is no single system that is the source for various PII that is stored on the GSS, the PII elements are described in each system's respective, governing System of Records Notice (SORN) and PIA.
14. If the information system is operated at more than one site, how will consistency of the information be ensured at all sites?	N/A

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.)	The retention schedule for each type of record varies. The CNCS offices are responsible for adhering to the CNCS and NARA record schedules for the PII stored on the GSS. As there is no single system that is the source for various PII that is stored on the GSS, the retention periods of PII will be in accordance with each system's respective, governing System of Records Notice (SORN) and PIA which identify the records schedules.
16. What are the procedures for disposition of the PII at the end of the retention period?	Physical paper is shredded and recycled. Electronic media is degaussed when decommissioned.
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?	The organization is implementing McAfee Data Loss Prevention. This tool has the capability to identify and track movement of PII within the boundaries of the GSS. Information will include users and activity.
18. Will the PII be retrieved using a personal identifier? List the identifiers that will be used to retrieve information and/or create reports.	No, PII will not be retrieved using a personal identifier.

MAINTENANCE AND ADMINISTRATIVE CONTROLS	
19. What controls will be used to prevent unauthorized monitoring or retrieval of PII?	Data center services, such as server services, middle-ware administration and support, system-level database administration and support and storage services are provided. Data network and security services include network managed services, secure point-to-point communications within the network, secure hosting environment, and IT components that comply with applicable Federal security and privacy mandates. All electronic data is encrypted at rest and in transit using FIPS 140-2 encryption protocols as well as user Identification with unique passwords, physical firewalls, external certificate authorities, auditing, web application firewall, and FISMA guidelines. Nessus is used for vulnerability scanning and Splunk is used for event correlation and logging. - Data is restricted to authorized users with CNCS roles and permissions; these authorized users have received and passed the required MBI Federal background clearance process. - For physical security: Security guards, close circuit cameras, Proximity ID badges and locked cabinets are used.

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.)	- CNCS offices (federal and contractor employees) who have placed the PII on the GSS will have read/write/delete to their files. - GSS System Administrators – Select employees that have been MBI/CBI cleared (received/passed a required federal background investigation). These users have READ, Write, Change access.

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.)	Limited PII is stored in the Network GSS in centralized storage as well as local storage on servers and user-dedicated systems. Use of centralized storage is governed by the CNCS Cybersecurity policy as well as the CNCS Rules of Behavior, which outlines employee roles and responsibilities. Directory structure and naming conventions are set up, and file permissions applied to directories and files. Individual staff and managers are responsible for proper storage, handling, and use of Agency data residing in individually assigned network storage space, and must comply with the CNCS cybersecurity policy, CNCS privacy policies and related records, retention, litigation, e-discovery, and information security procedures. Initial security training is conducted for new users and refresher training is conducted annually for all who have user accounts. The design and proper operation of the Network GSS is accomplished using current technology, including switches, routers, firewalls, monitors, and other equipment through which sensitive data may pass or be temporarily retained. Access to these devices is restricted to authorized network operations and operations assurance staff.
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?	Other systems do not have access to or share the PII.
23. Will the information be saved to removable media, or printed to hard copy? How will removable media and or hard copies be protected?	Tape backups are encrypted and stored using FIPS 140-2 compliance standards. Bins for the collection of printed PII are provided in copier rooms, and shredding is performed on a regular basis.

[i] CNCS SORNs and PIAs for eSPAN, Momentum, GMM, Childcare and health benefits system can be accessed on the NationalService.gov privacy policy page: http://www.nationalservice.gov/site-policy-and-notices/privacy-policy