Corporation for National and Community Service (CNCS) Privacy Impact Assessment (PIA)

1- GENERAL SYSTEM INFORMATION		
1-1	**Name of the information technology (IT) system:**	PRISM
1-2	**System Identifier (3 letter identifier):**	PRI
1-3	**Unique Investment Identifier (Exhibit 53):**	Not applicable to this system.
1-4	**Office or entity that owns the system:**	CNCS
1-5	**Office or entity that manages the system:**	Unison (vendor previously called CompuSearch)
1-6	**State if the system is operational or provide the expected launch date:**	Operational as of 1/4/2019
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:**	PRISM is a software application that is part of the CNCS General Support System (GSS), which is currently going through its annual security assessment.
1-9	**Approximate number of individuals with personally identifiable information (PII) in the system:**	PRISM contains information about the vendors who respond to CNCS solicitations and receive CNCS contracts. Over time, PII about 20,000+ individuals who do or want to work for or with those vendors (vendor staff members) may be included in that information; please see question 7-1 for additional details.

3- SIGNATURES (ORIGINAL MAINTAINED BY CHIEF PRIVACY OFFICER)		
	Role	***Electronic Signature & Date***
3-1	**System Owner:**	Signatures on file with Privacy Office
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 that CNCS developed for the 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.

5- SYSTEM PURPOSE	
5-1	**Describe the purpose of the system.**
	CNCS staff use PRISM to manage CNCS's procurement acquisition lifecycle to include planning the contract, developing the requisition, selecting the sources, awarding the contract, managing the delivery (e.g., tracking milestones and payment), and closing out the contract. Among other features, CNCS staff can: • Develop templates in PRISM to request the information needed for different types of transactions and the workflow to assure the correct CNCS staff give their approval • Upload documents to PRISM and link them to a solicitation or contract file and • Add notes to a solicitation or contract file and limit who can see the notes (e.g., a formal price comparison, an informal note to oneself about something in the file). PRISM connects to several other systems: • System for Award Management (SAM) is a Federal Government owned website that collects information about vendors who want to do business with the Federal Government. • beta.SAM.gov (previously FedBizOpps) is a Federal Government owned website where CNCS and other Federal agencies post certain solicitations so vendors can find them. • Federal Procurement Data System - Next Generation (FPDS-NG) is a Federal Government owned website where CNCS and other Federal agencies post information about certain awards for transparency purposes. • The Bureau of the Fiscal Service Invoice Processing Platform (IPP) is a Federal Government owned website that collects invoices from vendors requesting payment from CNCS and other Federal agencies. When IPP receives an invoice for CNCS, (a) IPP notifies PRISM, (b) PRISM notifies the CNCS staff member responsible for that invoice, (c) they approve, reject, or request to change the invoice in IPP, and (d) IPP notifies PRISM about that decision. • Momentum is CNCS's enterprise-wide financial management (i.e., accounting) system. When PRISM learns from IPP that an invoice has been approved or changed, it tells Momentum where those funds were spent. • FedConnect is another Unison run online service. Anyone can visit FedConnect and, without creating an account, view open solicitations from CNCS and other Federal agencies that use PRISM. Vendor staff who do create an account can (1) receive notifications when CNCS updates a solicitation, (2) view CNCS solicitations which are limited to certain

	vendors, (3) respond to a CNCS solicitation, and (4) accept a CNCS contract. FedConnect also has a messaging system; CNCS staff with PRISM accounts and vendor staff with FedConnect accounts can send each other secure messages and attachments about solicitations and contracts. • Unison Shared Services is Unison's General Support System which provides maintenance and security services to the system.

6- INVENTORY OF PII	
6-1	**Provide a list of all the PII included in the system.**
	The PII in PRISM includes names, business contact information (e.g., emails, phone numbers, physical addresses), and employment information (e.g., employer, job title, role). PRISM collects the Taxpayer Identification Number (TIN) for each vendor who registers in SAM. SAM system notifies users that their TIN will be shared with other systems. Even so, some small business owners choose to use their Social Security Number (SSN) as their TIN instead of acquiring a separate TIN for their business. Since the business owners choose to use their SSN as business information, PRISM handles and protects their SSN as business information.

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.**
	PRISM maintains PII about at least one vendor staff member for each vendor who responded to a solicitation, was awarded a contract, or was fulfilling a contract beginning in the fourth quarter of 2018. Over time, there will be PII about 10,000+ individuals in PRISM who fit this category. The proposals, contracts, and other acquisition documents collected and imputed into PRISM may include PII about additional vendor staff members who may support a contract. For example, a proposal to develop software could include information about the contract manager and the potential software developers. Over time, there will be PII about an additional 10,000+ individuals in PRISM who fit this category.

8- INFORMATION IN THE SYSTEM	
8-1	**For each category of individuals discussed above:** **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.**
	Each PRISM account includes the business contact information of one or more of the vendor's staff members (email, address, phone number); this information is collected from SAM, FedConnect, and other communications with the vendor. It may be linked to information about the vendor (e.g., TIN, location, business type, if indebted to the Federal Government) and information about any proposals, contracts, and other acquisition documents involving the vendor and CNCS. Those proposals, contracts, and other acquisition documents often include information about additional vendor staff members such as the:

	• business contact information of the individuals who would manage the contract • resumes of the individuals who would deliver the solution and • business contact information and references from past clients.

9- COLLECTIONS OF PII INTO THE SYSTEM	
9-1	**Describe for each source of PII in the system:** **a. The source.** **b. What PII comes from that source.** **c. How the PII enters the system.**
	All PII in PRISM is about vendor staff members and was provided by either the individual or another vendor staff member. The PII is entered into PRISM through one of three processes: • CNCS staff members receive the PII from outside PRISM (e.g., email) and then transcribe it into PRISM or upload the entire document into PRISM • PRISM imports the PII from SAM or • PRISM imports the PII from FedConnect.
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 <u>Not Applicable</u>.**
	Not applicable; only authorized CNCS staff members have direct access to PRISM.
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 <u>Not Applicable</u>.**
	Vendor staff members are aware that CNCS may (a) obtain their name, business contact information, and other employment-related information in the course of a proposal or contract and (b) store it in the system used to manage acquisitions. SAM is the system where all vendors must register to work with the Federal Government. SAM electronically provides to PRISM the name and business contact information of the vendor staff member who registered the vendor along with information about the vendor such as their TIN and whether they are barred from working with the Federal Government. The safeguards that help assure this PII is accurate are described in the SAM PIA located at: https://www.gsa.gov/reference/gsa-privacy-program/privacy-impact-assessments-PIA. Vendors who want to work with CNCS must also register with FedConnect. Once registered, they can use FedConnect to send PRISM responses to solicitations and messages which may contain PII. The FedConnect home page (https://www.fedconnect.net/) includes a tutorial that explains what information should be provided to FedConnect and how it will be used once collected. The FedConnect registration page has a link to the terms and conditions of the system which discuss the usage and sharing of the PII it collects.

9-4	**If any collections of PII 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 Not Applicable.**
	Not Applicable; the collections do not require an OMB Control Number.
9-5	**If any collections of PII into the system are subject to an agreement, describe those agreements. If no agreements are relevant, write Not Applicable.**
	Through the following agreements, PII is or will be collected into PRISM: a. An Interconnection Security Agreement (ISA) between CNCS and Unison because Unison hosts and maintains PRISM. b. An ISA between CNCS and Unison regarding FedConnect. c. An ISA between CNCS and Unison regarding Unison Shared Services. d. An ISA between CNCS and CGI Federal regarding Momentum. e. A Memorandum of Understanding (MOU) between CNCS and the General Services Administration (GSA) regarding SAM. f. A MOU between CNCS and GSA regarding beta.SAM.gov. g. A MOU between CNCS and GSA regarding FSDS-NG. h. A MOU between CNCS and the U.S. Department of Treasury, Bureau of the Fiscal Service regarding IPP.

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.**
	Approximately 15 CNCS authorized contract specialists and officers have access to PII on all vendors collected through PRISM. Those designated contract specialists and officers decide which CNCS personnel shall have access to the PII regarding a solicitation or contract. Approximately 61 other authorized CNCS staff members whom are associated with the acquisitions process have authorized access to different segments of PRISM. Those CNCS staff members may be responsible for completing requisition requests, analyzing the budget, or approving purchases. Approximately 20 Unison staff members have authorized access to CNCS information within PRISM to help manage the system. The Unison Shared Services System Security Plan (SSP) specifies the level of access and privilege level each Unison staff member receives based on their role.

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.**
	PRISM electronically connects to IPP, Momentum, beta.SAM.gov, SAM, and FPDS-NG, but PRISM does not share any PII about vendors staff members with those other systems. PRISM electronically connects to FedConnect to enable CNCS and vendor staff members to send and receive secure communications about a solicitation or award. These communications could include any of the PII described in 8-1. FedConnect is designed so only one vendor staff member should have access to information about that vendor. The privacy policy for FedConnect is located at https://www.fedconnect.net/FedConnect/marketing/privacy.htm. CNCS also has an ISA with Unison which discusses the privacy and security requirements that must be in place to retain this connection. All communications to and from PRISM are protected via either AES-256 encryption or TLS v1.2 encryption over HTTPS.

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 system of records notices (SORN) applies 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 technical, physical, and administrative safeguards that protect the PII in the system.**
	PRISM is a FedRAMP authorized cloud-based software as a service (SaaS) application with a Federal Information Processing Standard (FIPS) 199 categorization of Moderate. A comprehensive security plan helps protect PRISM from potential attackers, unauthorized connections, system flaws, and other vulnerabilities. Every year, PRISM undergoes a complete assessment of all security requirements listed in NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; any unmet requirements are tracked and reviewed on a regular basis. PRISM also undergoes continuous monitored consistent with NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations. Scanners autonomously review system activities for potential attacks. Regular and ad hoc system scans search for potential vulnerabilities. Unison's authorized staff members regularly review audit logs which capture a

	broad range of system activities including changes to the data, changes to a user's access, and login attempts. Unison's authorized staff members receive the least amount of PRISM access needed based on their role. Unison's authorized staff members regularly review whether that level of access remains necessary. All authorized Unison staff members and contractors sign a rules of behavior document and non-disclosure agreement before receiving that access, plus regularly complete an IT Security Awareness Training. Those with elevated system access also regularly complete a Privilege Administrators Training. Controls regarding CNCS staff members with access to PRISM are described in the General Support System PIA. PRISM's physical servers reside in a secure facility and are regularly checked to assure the individuals who have access to those servers require access. PRISM has an incident response plan which establishes how all CNCS and Unison staff members should identify, contain, eradicate, and recover from an information security incident. Key staff members sporadically complete a table top exercise to practice that plan. All communications to or from PRISM are protected via either AES-256 encryption or TLS v1.2 encryption over HTTPS.

14- DATA ACCURACY, ACCESS, AMENDMENT, AND CONTROL	
14-1	**Describe the steps taken to ensure PII is sufficiently accurate, relevant, current, and complete.**
	All PII inputted into PRISM is originally sourced from a vendor staff member who provides PII about themselves or another vendor staff member. Any vendor staff members whose name and business contact information were transferred from FedConnect or SAM to PRISM can login to their FedConnect or SAM account at any time and update their PII; within a short amount of time PRISM receives the new information and updates their account. PRISM frequently checks whether the PII in FedConnect and SAM are different, then informs CNCS so they can investigate the discrepancy.
14-2	**Describe how an individual could view, correct, update, or ask to amend their PII.**
	Any vendor staff member could contact a CNCS contract specialist or the CNCS Privacy Office regarding inaccurate PII, but CNCS's ability to modify the PII depends on its purpose. For example, CNCS may not be allowed to change a proposal after submission because it contains inaccurate PII.
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.**
	Each vendor can decide what PII they want to include about their staff; if a vendor staff member does not want their PII listed in PRISM, the vendor could list someone else or decide not to contract with CNCS.

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.**
	PRISM stores PII linked to an acquisition for up to 7 years after the final action is taken. At the conclusion of the contract between Unison and CNCS, CNCS has the option to receive a full copy of the acquisition information including all PII. CNCS is currently working to develop a complete NARA approved records retention and disposal schedule for PRISM. Until it is approved, all records in PRISM are retained and none of them are disposed. Once the NARA record schedule is approved, all records in PRISM will be retained and disposed according to that 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; PRISM does not specifically ask for any SSNs and CNCS does not treat TINs as SSNs.

17- WEBSITES	
17-1	**If the system includes a website which is available to individuals apart from CNCS personnel and contractors, discuss how it meets all CNCS and Federal privacy requirements. If the system does not include a website, write Not Applicable.**
	Not applicable; PRISM is only available to CNCS personnel from the CNCS network.

18- OTHER PRIVACY RISKS	
18-1	**Discuss any other system privacy risks or write Not Applicable.**
	Not applicable.