ATTACHMENT I – PROJECT TOPIC

Secure Compute Environment Testbed for a National Secure Data Service

Purpose

The purpose of this project is to design and build a secure compute environment testbed that will be leveraged as part of an overall effort to build a linkage and access infrastructure to support the NSDS-D. This compute environment will increase NSDS-D abilities to process and analyze data, maintain data security, and expand research access as well as serve as a testbed for an infrastructure for a potential NSDS. This environment will also allow us to implement testing of privacy-preserving technologies as required under Section 10375 of the CHIPS and Science Act. This project will test the required infrastructure for the activities under an NSDS-D.

Background

The CHIPS and Science Act, PL 117-162, was signed into law in August 2022. Section 10375 establishes a National Secure Data Service Demonstration Project (NSDS-D) to "develop, refine, and test models to inform the full implementation of the Commission on Evidence-Based Policymaking recommendation for a governmentwide data linkage and access infrastructure for statistical activities conducted for statistical purposes, as defined in chapter 35 of title 44, United States Code."

Per the CHIPS and Science Act Section 10375(b)(2), the NSDS-D will be "operated directly by or via a contract that is managed by the National Center for Science and Engineering Statistics." The National Center for Science and Engineering Statistics (NCSES, a Federal Recognized Statistical Agency) within the National Science Foundation (NSF, the Foundation), conducts surveys and other data collections and provides data and analyses about the Nation's activities and resources in science and engineering (S&E). Customers include government, education, and industry officials and others engaged in funding, conducting, or managing R&D; S&E education; the S&E workforce; or the reporting of issues related to science, engineering, and technology. The work of NCSES and its wide range of stakeholders' positions NCSES well to serve as the Project Management Office (PMO) for the NSDS-D.

A key element in the legislation is data security through the use of privacy-preserving technologies. The ability to establish a shared IT environment that can be leveraged for use by multiple government entities is critical as is the use of the environment for the testing of novel privacy-preserving technologies and data linkage techniques. Data used within this environment would be subject to privacy and confidentiality restrictions within multiple statutes including, but not limited to, the Privacy Act of 1974, as amended; the Confidential Information Protection and Statistical Efficiency Act of 2018; the National Science Foundation Act of 1950, as amended; Title 13, U.S.C.; Title 26, U.S.C.; Title 42 U.S.C.; the Family Educational

Rights and Privacy Act (FERPA); and the Health Information Portability and Accountability Act (HIPAA). These statutes provide for the security and privacy of individually identifiable statistical data maintained by NCSES as well as other statistical agencies within the Federal Government. Sections of these laws make unlawful the willful disclosure or improper use of data containing individually identifiable information, and subject to a fine and/or imprisonment. Other statutes may apply under certain circumstances, such as the Computer Fraud and Abuse Act of 1986, which makes it a felony to gain unauthorized access to a computer system containing Federal data, or to abuse the access one has, with the purpose of doing malicious destruction or damage.

Objectives

The requirements for the Secure Compute Environment Testbed project are detailed in the accompanying Statement of Work (Enclosure 1 below).

Offerors should propose tasking and associated costs in three (3) phases outlined below. Time ranges are estimates and offerors can propose modifications.

- Phase 1 - Build the Secure Compute Environment Testbed (~3 months or less)
- Phase 2 – Operational Testing of the Secure Compute Environment Testbed (~2 months or less) – estimate 100 users for the duration of Phase 2 (government and non-government)
- Phase 3 – Demonstrate/Enhance the Secure Compute Environment Testbed (through August 9, 2026) – estimate 500 users for the duration of Phase 3 (government and non-government)

All contractors with access to the compute environment will be required to become designated CIPSEA agents and take annual CIPSEA training. Additional security requirements for contractors may be necessary depending on the data used within the environment.

If there are existing tools, software, and technologies that can achieve the stated goals of the Secure Compute Environment Testbed, then the offeror should use them and avoid developing custom-built tools, software, and technologies. If new tools are required, the Secure Compute Environment Testbed offeror should provide a clear explanation for why existing technologies in the market are insufficient. All technology and software developed should be easily portable with minimal constraints imposed by proprietary software, and have suitable APIs for plug and play and be transferable at the conclusion of the contract.

If any information technology (IT), websites, and/or cloud technologies are procured or developed as a part of the Secure Compute Environment Testbed effort, then the offeror must ensure that these solutions comply with NSF and/or federal IT security, information management, and data security requirements. Coordination with NSF's Division of Information Systems (DIS) may be required as well as other Offices of Security at federal agencies, as needed.

Deliverables

At a minimum, offerors will provide the following if selected for award. Additional deliverables may be required.

- Bi-weekly meetings with NCSES program staff. This will include establishing meetings, agendas, and taking meeting minutes.
- Monthly reports, following the template provided by ATI, including quarterly lessons learned highlighting key lessons learned for the quarter. As this is a testbed for potential development of infrastructure for an NSDS, understanding successes, challenges, and opportunities will be critical to inform future development.
- A final report that includes work completed and a compilation of lessons learned from the full performance period.
- All security and FedRAMP documentation listed in section 1.3.2 of the SOW.

Enclosure 1 – Statement of Work

1.0 Description of Services

1.1 Background

The CHIPS and Science Act, PL 117-162, was signed into law in August of 2022. Section 10375 establishes a National Secure Data Service Demonstration Project (NSDS-D) to 'develop, refine, and test models to inform the full implementation of the Commission on Evidence-Based Policymaking recommendation for a governmentwide data linkage and access infrastructure for statistical activities conducted for statistical purposes, as defined in chapter 35 of title 44, United States Code.'

Per the CHIPS and Science Act Section 10375(b)(2), the NSDS-D will be 'operated directly by or via a contract that is managed by the National Center for Science and Engineering Statistics'. The National Center for Science and Engineering Statistics within the National Science Foundation (NSF, the Foundation), a Federal Statistical Agency, conducts surveys and other data collections and provides data and analyses about the nation's activities and resources in science and engineering. Customers include government, education and industry officials and others engaged in funding, conducting, or managing R&D; science and engineering (S&E) education; the S&E workforce; or the reporting of issues related to science, engineering, and technology. The work of NCSES and its wide range of stakeholder positions NCSES well to serve as the Project Management Office (PMO) for the NSDS-D.

A key element in the legislation is data security through the use of privacy-preserving technologies. A shared IT environment that can be leveraged for use by multiple government entities is critical as is the use of the environment for the testing of novel privacy-preserving technologies and data linkage techniques. Data used within this environment would be subject to confidentiality restrictions within multiple statutes including, but not limited to, the Privacy Act of 1974, as amended; the Confidential Information Protection and Statistical Efficiency Act of 2018; and the National Science Foundation Act of 1950, as amended; Title 13, U.S.C.; Title 26, U.S.C.; Title 42 U.S.C.; the Family Educational Rights and Privacy Act (FERPA); and the Health Information Portability and Accountability Act. These statutes provide for the security and privacy of individually identifiable statistical data maintained by NCSES as well as other statistical agencies within the Federal Government. Sections of these laws make unlawful the disclosure or improper use of data containing individually identifiable information, and subject to a fine and/or imprisonment. Other statutes may apply under certain circumstances, such as the Computer Fraud and Abuse Act of 1986, which makes it a felony to gain unauthorized access to a computer system containing Federal data, or to abuse the access one has, with the purpose of doing malicious destruction or damage.

1.2 Scope

The purpose of this project is to design, deploy, and support a secure compute environment testbed that will be leveraged as part of an overall effort to build a linkage and access infrastructure to support the NSDS-D. This secure compute environment testbed will increase our abilities to process and analyze data, maintain data security, and expand research access. This environment will also allow us to implement testing of privacy-preserving technologies as required under Section 10375 of the CHIPS and Science Act. This project will test the required infrastructure for the activities under an NSDS-D.

1.3 Statement of Work

1.3.1 Project Management

The contractor will provide project management to oversee the successful completion of all tasks in the statement of work.

1.3.1.1 Planning (roadmap)

Within 1 month after the contract has been awarded, the contractor shall provide the Contracting Officer Representative (COR) a roadmap for this contract. The contractor will develop project-specific milestones and schedules. The contractor will provide monthly updates on the status of NCSES's desired milestones and goals. The contractor will provide quarterly and an annual presentation to the COR and NCSES Leadership to outline past year outcomes and upcoming quarterly or yearly milestones and goals.

1.3.1.2: Risk management

The contractor will produce a risk management plan and maintain and review projects, schedules and resources and report risks on a monthly or time-sensitive basis that impact the overall project and how to avoid and/or correct it. The plan must include identification of risks, an assessment of probability of occurrence and impact, risk management, and risk reporting and monitoring.

1.3.1.3 Documentation

The contractor will draft and maintain technical documentation for all products developed in this project. Documentation shall be delivered with every major product release and approved by the NCSES COR

1.3.1.4 Communication management

The contractor will propose and implement a communication plan outlining a communication protocol in at least the following areas: status meetings and reports, system documentation, system monitoring and reporting, and interacting and coordination with NCSES staff and contract-related personnel. As needed, the contractor will work with the COR and other key staff to suggest communication strategies to alert, inform, coordinate, update and brief NCSES staff, including Leadership, on any new or ongoing projects and initiatives. The communication plan will need to be delivered within the first 6 months of contract award. COR approval of the plan is required.

1.3.1.5 Financial management, resources and procurement of hardware and software

The contractor will manage the contract budget and maintain a detailed financial record of their costs. The contractor will propose a financial management plan, including and a proposal for a monthly financial report to the COR. The monthly financial report will include, at a minimum, the monthly break-down of the actual labor costs, projected labor costs, and other direct costs for the entirety of the contract. The contractor is required to notify the COR when 75% of obligated funds have been spent. The financial management reports will be incorporated in the monthly, quarterly, and year-end deliverable. The contractor will work with the COR and NCSES staff to identify requirements and manage the procurement of software and services needed for this work. The contractor will also propose a resource plan, included in the proposal submission, that includes staffing and other resources needed to achieve NCSES milestones goals and known projects within a month of the contract start date.

1.3.1.6: Transition activities

To ensure the smooth transition-out of the project to a potential new contractor at the end of this contract, the contractor will develop and execute a COR approved transition-out plan for the project to a new contractor. This plan will be delivered 6 months before the expected end of the contract.

1.3.1.7: Security Clearances

To ensure compliance with all data confidentiality requirements, including the Confidential Information Protection and Statistical Efficiency Act (CIPSEA). All contractors with access to the compute environment will be required to become designated CIPSEA agents and take annual CIPSEA training. Additional security requirements for contractors may be necessary depending on the data used within the environment.

1.3.2. Secure Compute Environment Testbed

The Contractor will accomplish the following activities at a minimum to build and maintain the Secure Compute Environment Testbed.

- Establish a secure, scalable, transferable, cloud based (FedRAMP Moderate Impact Level) compute environment (housed on U.S. servers only) in which data can be linked and utilized for statistical purposes.
    - The contractor shall leverage existing FedRAMP Authorized cloud service(s) at the Moderate Impact Level.
    - The contractor shall confirm implementation of controls contained within the FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements for moderate impact systems (as defined in FIPS PUB 199).
    - The contractor shall create, maintain, and update the following documentation using FedRAMP requirements and templates (https://www.fedramp.gov/) to support the agency Authority to Operate (ATO) process:
        - Privacy Impact Assessment (PIA)
        - FedRAMP Test Procedures and Results
        - Security Assessment Report (SAR)
        - System Security Plan (SSP)
        - IT System Contingency Plan (CP)
        - IT System Contingency Plan (CP) Test Results
        - Plan of Action and Milestones (POA&M)
        - Continuous Monitoring Plan (CMP)
        - FedRAMP Control Tailoring Workbook
        - Control Implementation Summary Table
        - Results of Penetration Testing
        - Software Code Review
        - Interconnection Agreements/Service Level Agreements/Memorandum of Agreements
    - Develop and maintain FedRAMP documentation for an Authorization package (See the Excel sheet for FedRAMP-Initial-Authorization-Package-Checklist.xlsx (live.com).
    - Selects a Third-Party assessment Organization (3PAO) to conduct independent assessment of controls on place for the ATO and annually thereafter (required by FedRAMP).

    - Following the ATO, maintain continuous monitoring and produce documentation for 3PAO and Federal review (scanning results, POA&M, annual assessments, etc.). See the CSP Authorization Playbook - Vol. I & II (fedramp.gov) for a full description of service provider and Federal staff responsibilities during the authorization process.
- Ensure the ability to securely partition project spaces to restrict access to groups of datasets by an approved set of users.
- Implement security controls to prevent insertion and removal of data and output from the environment by users without permission by designated individuals. Insertion of external data into project environments will be possible with the permission by government-designated individuals.
- Provide logging of user actions and production of audit logs to monitor suspicious behavior and security threats.
- Populate the environment with SAS, Stata, SUDAAN, R, and Microsoft Office Suite software for use by approved users to analyze data via statistical methods including, but not limited to, hypothesis testing, regression, correlation analysis, and cross tabulations. Python and Java should also be made available for the same purpose. Additional software (Tableau, Spark) may be needed as directed by the government.
- Maintain latest version/security patches on all software to be updated at least once a month.
- Ensure the ability to utilize homomorphic encryption tools for Privacy Preserving Record Linkage (PPRL), secure multi-party computing platforms, and potential linkage to validation servers.
- Ensure a compute capacity to manipulate large datasets with records of 100M+ and 1000+ unique columns or variables.
- Provide for archiving of project spaces for a time period specified by NCSES, but not to exceed the period of performance of this contract. Transfer of archived project spaces must be included in the transition plan.

1.3.3. Secure Compute Environment Testbed support

In addition to creating this environment, we require the offeror to maintain the environment and provide customer support in establishing project spaces and supporting user access, user training, and "helpdesk" support. The contractor shall propose training activities aligned with industry best practices.

1.3.3 System Support tasks

1.3.3.1 System Administration

The Contractor will, at a minimum, conduct the following activities:

- Deploy system buildout/setup/updates, configuration changes, and patches.
- Support validation activities (testing/approving).
- Monitor system status and security scan results, and respond as needed.
- Offerors should propose an approach that maximizes up time, including having a back-up system administrator.

1.3.4 Section 508 of Rehabilitation Act and general accessibility

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when federal agencies develop, procure, maintain, or use information and communication technology (ICT), it will be accessible to people with disabilities. Federal employees and members of the public who have disabilities must have access to, and use of, information and data that is comparable to people without disabilities.

Products, platforms and services delivered as part of this performance work statement that are ICT, or contain ICT, must conform to the Revised 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. A, C & D, and available at https://www.access- board.gov/guidelines-and-standards/communications-and-it/about-the-ict- refresh/final-rule/text-of-the-standards-and-guidelines.

1.4 Places of performance and work conditions/hours

The place of performance and work conditions and hours are to be determined by the Contractor. No work will be performed outside the United States, including accessing government data and email. Any government-provided equipment cannot be taken outside of the United States. The period of performance is the time from award through August 9, 2026. The base period will be from the time of award through the first 12 months. Each subsequent option period will last 12 months with the final option period lasting the remainder of the contract period through August 9, 2026.

1.5 Key Personnel

Key personnel to be included for this project must include:

- Project Leader
- Project manager
- Task Leads (as proposed)

Identify and describe the capabilities and experience of key personnel and organizations as these elements relate to the proposed project. Descriptions of experience should serve to demonstrate the key personnel's ability to successfully conduct the proposed research or project, including access to critical resources for the project. Designate any supervisory relationships and who will be the main point of contact for regular check-ins with the NCSES methodological team during the project. Provide condensed resumes (2-page maximum) for all key personnel on the project. Resumes shall be organized in an appendix to the proposal. Resumes do not count toward the 20-page limit for the proposal.

In addition to key personnel, designate any graduate students or postdoctoral fellows funded by the proposed research. If named, provide no more than a half-page biographical sketch of their background and research interests. The biographical sketch should be included as part of the resume appendix and does not count against the page limit.

Describe any unique capabilities that the offeror team possesses that may reduce project risk, reduce project duration, and/or improve project financial performance.

Additional Information

The offeror will be expected to support this compute environment, serving as a test bed, for the National Secure Data Service demonstration project through August 9, 2026.

All contractor staff with access to the compute environment will be required to become designated Confidential Information and Statistical Efficiency Act (CIPSEA) agents and take annual CIPSEA training.

Additional security clearance requirements (such as Special Sworn Status) for contractors may be necessary depending on the data used within the environment.

If there are existing tools, software, and technologies that can achieve the stated goals of the Secure Compute Environment Testbed, then the offeror should use them and avoid developing custom-built tools, software, and technologies. If new tools are required, the offeror should provide a clear explanation for why existing technologies in the market are insufficient. All technology and software developed should be easily portable with minimal constraints imposed by proprietary software and have suitable APIs for plug and play.

If any information technology (IT), websites, and/or cloud technologies are procured or developed as a part of the Secure Compute Environment Testbed effort, then the offeror must ensure that these solutions comply with NSF and/or federal IT security, information management, and data security requirements. Coordination with NSF's Division of Information Systems (DIS) may be required as well as other Offices of Security at federal agencies, as needed.

One copy of each report will be submitted to the client representative. The contractor will deliver each report in a mutually agreed upon format. Deliverables are to be transmitted with a cover letter, on the prime contractor's letterhead, describing the contents.

Only the client representative (CR), their designated alternate, the Project Manager (PM), the Contracting Officer's Representative (COR), or Contracting Officer (CO) has the authority to inspect, accept, or reject all deliverables. Final acceptance of all deliverables will be provided in writing, or in electronic format, to the PM or CO within 30 days from the end of the task order.

The contractor will establish and maintain a complete Quality Control Plan (QCP) within 60 calendar days of contract award to ensure the services are performed in accordance with PWS and commonly accepted commercial practices. Strategies for quality control should be included in the proposal submission. The contractor will develop and implement procedures to identify, prevent and ensure non-recurrence of defective services. The government reserves the right to perform inspections on services provided to the extent deemed necessary to protect the government's interests. The contractor must control the quality of the services and deliverables provided in support of this project and maintain substantiating evidence that services conform to contract quality requirements and furnish such information to the government if requested. The QCP will include a quality control matrix (QCM). The QCM will reflect the quality approach of the vendor as it applies to the key areas of the offeror's proposed TA.

Contract Line Items (CLIN) and Contract Type

CLIN 0001 (Firm Fixed Price) 1.3.1 Project Management

CLIN 0002 (Expenditure Based) 1.3.2. Secure Compute Environment Testbed

CLIN 0003 (Expenditure Based) 1.3.3. Secure Compute Environment Testbed support

Optional Surge CLIN (Expenditure Based) – Not-to-Exceed $500,000

An option CLIN for surge is intended to be included in the task order for unanticipated increases in users and user support. The CLIN would be priced based on the size of team, or ramp-up of current team to accommodate such workload. Pricing for small, medium, and large teams or equivalent ramp-up should be provided. The Option CLIN would be included in the award based on the pricing submitted with a Not-to-Exceed value that could be exercised in the event the need exists and the funds become available.