ATTACHMENT I – PROJECT TOPIC

Secure Compute Environment Environmental Scan

Key Objective

The objective of this project is to understand the current landscape of secure computing environments within the federal government as they pertain to data sharing and privacy and confidentiality restrictions within multiple statutes, to help inform a potential National Secure Data Service. This scan will include compiling legal requirements under different statutes for data protection and security, as they relate to IT infrastructure to store and utilize confidential data.

Background

The CHIPS and Science Act, PL 117-162, was signed into law in August 2022. Section 10375 of the Act authorizes 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 research and development (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 using 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 (CIPSEA) 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.

Understanding the landscape of secure computing and privacy and confidentiality statutes will help inform the establishment and ongoing development of a Secure Compute Environment for the NSDS demonstration project and a potential future NSDS.

Objectives

The objectives for the Secure Compute Environment environmental scan include:

1. Explore the IT data infrastructures (e.g., secure computing environments, data lakes, etc.) that have been established or are in the process of being established by federal statical agencies and potentially other data holding agencies. This scan will include considerations based on differing privacy and confidentiality statutes at the respective agencies.
2. Produce findings that will include but are not limited to how other agencies have securely partitioned project spaces to restrict access to groups of datasets by an approved set of users, how they have implemented security controls to prevent insertion and removal of data and output from the environment by users without permission by designated individuals and the ability to deploy homomorphic encryption tools for Privacy Preserving Record Linkage (PPRL), secure multi-party computing platforms, and potential linkage to validation servers with a secure compute environment. In addition, produce an analysis of what types of services and software other agencies are providing on their secure computing platforms.
3. Explore the computing capacities that are required to manipulate large datasets and identify what is working and what is not.
4. Explore the capabilities of agency systems to archive project spaces for a time period in a secure compute environment and how it is implemented.
5. Compile legal requirements under existing statutes, including FISMA and data confidentiality statutes, that relate to IT infrastructure requirements.

Information Gaps

This project will identify key components necessary to inform a future/potential NSDS including:

- The key components needed to develop a Secure Compute Environment that can be used for data sharing, linkages, analyzing data while adhering to privacy and confidentiality statutes.

Deliverables

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

- A final summary report with recommendations for establishing a Secure Compute Environment in support of a potential NSDS.