Appendix A-2. Data Security Protocols

Data management security protocols ensure restricted access to data and confidentiality of data maintained in information systems and in reports. The contractor, uses secure intranets to maintain project-related files, and its secure servers employ industry-standard methods, such as firewalls, monitored-access logs, virus protection, encrypted connections, password-protected accounts, and user-authentication mechanisms, to ensure the confidentiality of the data collection, test data, and subsequent analyses. Its security protocols were designed to fulfill obligations of the Privacy Act and Office of Management and Budget (OMB) circulars and memorandum.

System Environment
The security approach used to protect Sensitive But Unclassified (SBU) or proprietary business data is based upon Defense in Depth principles. Security protections have been designed to address controls relative to people, technologies, and operations, with technologies focused on defending the network or perimeter, the enclave, the computing environment, and the supporting structures. Whether through a vendor or locally hosted, the system environments meet best practices for physical and environmental controls as outlined by the National Institute of Standards and Technology (NIST). For example, power continuity is provided through redundancies to ensure that back-up power systems will provide ample capacity to keep servers running during any generator failure; signed access rights forms are required for changes to the limited staff assigned to each project and system.

File Transfer
The contractor uses a range of proven file transfer methods, depending on the requirements of the project. Cryptographic protocols, such as Secure Socket Layer (SSL) or Transport Layer Security (TLS), are in place, and a minimum of AES 256 encryption is used. Protocols meet standards established by Federal Information Processing Standard (FIPS) publication 140-2. End users can connect to servers using a variety of secure file transfer protocol (FTP) clients or other interfaces. Each user has a unique username and password and only has access to his or her project data. Access logs are kept for security review purposes.

Secure Servers
The contractor operates several secure servers to meet the data security needs of various projects. These servers are protected using industry standard methods, such as firewalls, monitored-access logs, virus protection, encrypted connections to each server, and passwords that must be changed every 90 days. Data can be analyzed using statistical packages and other applications located on each server, eliminating the need to move the data to an unsecure location. The STATA and R software, for example, are running in a remote, secure, virtual environment. These software programs can be used to analyze and report on a wide variety of datasets. Running on remote servers allows the data to be analyzed from a single location. All unused and unnecessary services are disabled on the servers.

In cases where data cannot be maintained on a network, the necessary software is installed for use on a stand-alone PC without a connection to the Internet. It may allow access to a local server and/or allow physical access to the room, depending on the requirements of the project.