SSS Data Security Standards

SSS considers information security as an integral requirement and has, in principle, adopted the Federal Government model of computer security. We acknowledge that security plans are required for all Federal automated information systems and systems operated by contractors to the Federal Government. The enabling legislation that requires plans is Public Law 100-235, Computer Security Act of 1987 (now superseded by the Federal Information Security Management Act [FISMA] of 2002), and the regulation, promulgated from this legislation, is the Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, especially Appendix III.

The National Institute of Standards and Technology (NIST), within the Department of Commerce, is responsible for developing security plan standards. NIST special publication 800-18 entitled, "Guide for Developing Security Plans for Information Technology Systems," incorporates the requirements of the Computer Security Act and OMB Circular A-130. This security plan closely follows these NIST guidelines.

SSS is knowledgeable of the security requirements outlined in Appendix III of OMB circular A-130. SSS will follow these requirements, as well as address the security objectives of confidentiality, integrity, and availability outlined in the FIPS publication 199 guidelines while performing tasks under this contract. Project staff will comply with the HHS Rules of Behavior set forth in HHS Information Security Program Policy Handbook, Appendix G. Following is an example of specific technical and managerial controls implemented by SSS to ensure security:

A. Managerial Controls
    - All SSS employees are currently required to complete the NIH Security Awareness Training.
    - Notify the project director when unauthorized use is suspected
    - Maintain the confidentiality of all passwords and notify the project director when any changes are made to a password
    - When confidential information is needed to link to other data, follow the same security procedures for confidential data
    - Store all confidential materials (tapes, disks, paper) in the designated secure storage room at SSS
    - Do not take confidential materials home — use of confidential files is prohibited at home
    - Do not leave confidential data unattended
    - Shred confidential printouts when they are no longer needed
    - Backup key data files and program libraries as specified by project backup standards. Our network backups include offsite storage.

B. System Controls

SSS Staff and system users are required to:

- Choose passwords that are not easy to decipher—e.g., mixed-cased alphabetic, non-alphabetic (numbers, punctuation).
- Change passwords at least every 90 days
- Not use common names, telephone extensions or numbers, birthdates, or other commonly available information for passwords.
- Not use common dictionary words for passwords.

SSS systems managers, administrators, and developers are instructed to:

- Configure software, servers, and systems to require that users change passwords every 90 days.
- Have administrator-level passwords change every 60 days, for systems containing secure data or information and every 90 days for others.
- Perform vulnerability scans on systems following application enhancements or application of system updates.

SSS Project Managers are instructed to:

- Develop, post, and enforce a password policy that is compliant with this policy for project-specific data and systems.
- Consider a more rigorous policy towards passwords for software and systems with extremely sensitive information such as patient records. Stronger authentication through technologies such as encryption, biometrics, or smart cards may be warranted in some instances.

C. Physical Controls

- The building at 8757 Georgia Avenue in Silver Spring, Maryland is controlled and monitored by Datawatch Systems, a full-service access-control security services company. Datawatch Systems is recognized as one of the top security system integrators in the nation.
- Access to the building during working hours is monitored by an onsite security guard. Outside of normal working hours, a Datawatch access card is required to operate the elevators and open the access doors. Once in the building, access to SSS premises is controlled by the Datawatch system and is available only to SSS personnel in possession of a Datawatch Systems (Silver Spring) card.
- Visitors are directed to the reception desk on the 12th floor, are required to sign in and out using the visitor log, and are provided a Visitor's badge and are escorted while in SSS space.
- Access to all floors and suites that SSS occupies is controlled by Datawatch’s access control systems that utilize a proximity card. Each

card will only allow a person to access areas for which they have been previously approved. Each use of the card to open an access door is logged.

- SSS server rooms, network labs, console rooms, and project rooms are secured by cipher locking mechanisms on all entrances. Only authorized personnel possess the means to enter these rooms by way of the locking devices. The codes to the network lab, console room and datacenter are changed every 6 months or more frequently as deemed necessary. An access log is maintained in the datacenter to record each visit.

- SSS controls physical access to information system transmission lines carrying unencrypted information to prevent eavesdropping, in-transit modification, disruption, or physical tampering. All cables are contained within SSS-controlled areas of the building and terminate in SSS-controlled space.

- External services are secured in the building's main telecommunications room and carried on SSS-owned and maintained cabling through risers to SSS' own telecommunications rooms.

- Visitors doing business with the SSS are not permitted access to secure areas containing computer systems, files and other confidential data. When it is occasionally necessary for visitors, or the firm's employees without the required clearance to enter the area, they will be accompanied by an authorized SSS staff member. Visitors will not be permitted to observe computer workstation displays or have visual access to reports or other confidential information. Visitors will remain in the secure area only long enough to perform the required activity which made it necessary for them to enter. Visitor access to the secure datacenter housing project systems will be documented in a logbook containing name, visiting person's organization name, reason for access, date, time and identification of the SSS staff person present during their visit.

- Visitors to SSS spaces are required to sign in and out at the building's 12th floor SSS receptionist. A visitor log that consists of date, name, company, time in, time out, person visiting and SSS internal badge number are maintained by SSS and reviewed by designated SSS personnel. Access records for all staff, contractors, and temporary staff are retrievable through records maintained by SSS' access control security providers.

D. Power Equipment

- SSS has an emergency power generator that is serviced on a regular basis. SSS maintains a service contract for the power generator. The generator is located in the building's access-controlled garage and surrounded by a security fence. SSS permits only authorized Maintenance personnel to access the power generator and power cabling.

- For specific locations within a facility containing concentrations of information system resources SSS provides the capability of shutting off power to any information technology component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without endangering personnel by requiring them to approach the equipment.

- SSS provides a short-term uninterruptible power supply (UPS) to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

- SSS provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

- The building at 8757 Georgia Avenue in Silver Spring, Maryland is managed by Washington Property, who ensures that the emergency lighting is operational during power outages and covers emergency exits per the county code. Lighting is strategically placed for this purpose throughout the facility.

E. Fire Protection and Environmental Controls

- The building at 8757 Georgia Avenue in Silver Spring, Maryland is managed by Washington Property Company. Washington Property Company building engineers are responsible for the operation and maintenance of fire detection/fire suppression devices. These devices provide automatic notification in the event of a fire and such notification is transmitted immediately to designated SSS personnel. The current fire suppression for this building is a water sprinkler system. Additionally, fire extinguishers are strategically located under SSS control in the server room and in all project rooms and console rooms. Fire extinguishers are inspected semi-annually and are either ABC Dry Chemical or C02 Carbon Dioxide.

- SSS has monitoring units in all control rooms and project rooms to track and report on the temperature and humidity in the areas. Alerts are initiated if any of the measurements exceed acceptable operating parameters. Contracts with vendors for HVAC and other services provide the requisite service as needed

- Washington Property Company's building engineers are responsible for accessing and operating (if required) master shutoff valves. These valves are accessible on each floor, frequently tested, and their location is noted in floor plans available to key SSS personnel.