Westat

Improving Lives Through Research®

Data Security Plan

Final

Date: June 13, 2025

Submitted to:
Agency for Healthcare Research and Quality
Rockville, MD

Submitted by:
Westat
An Employee-Owned Research Corporation®
7501 Wisconsin Avenue, Suite 1000E
Bethesda, MD 20814
(301) 251-1500

Table of Contents

Table of Contents

Exhibits

1. Overview and Organization of the Plan

The data security plan describes the security procedures implemented for the Household Component (HC) of the Medical Expenditure Panel Survey (MEPS). Implementing data security procedures for this survey implies both safe transmission of data and its confidentiality requirements. The data must be protected not only from unintentional destruction or alteration, but from disclosure through unauthorized access as well. Confidentiality is of particular concern because the MEPS collects both Protected Health Information (PHI) and Personally Identifiable Information (PII), such as respondents' personal history, medical conditions, insurance coverage, income and financial status. These data are protected by Federal regulations including the Privacy Act and the Public Health Service Act (see section Exhibit 1-2). The data security procedures and guidelines implemented for MEPS are based on an understanding of confidentiality as required by the legislation guiding the study and federal regulations for HHS confidential data and OMB Circular A-130.

Westat develops and operates all systems in conformance with the standards set forth by the Federal Information Security Management Act (FISMA) and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*. This activity is ongoing and documentation is updated when a major change occurs to the system, and reviewed annually. The Westat AHRQ Project Support System (AHRQ-PSS) Security Assessment and Authorization (SA&A) package is compliant with all Public Law (PL)-107-347, OMB mandates, FIPS, and additional applicable NIST guidance.

The HHS SA&A checklist is used in the development of the SA&A materials. Prior to becoming operational, all systems receive a signed Authorization to Operate (ATO) issued by AHRQ's Designated Authorization Authority (DAA). MEPS is part of the AHRQ-PSS that last received an ATO from AHRQ on June 14, 2024. Westat meets ongoing information security and privacy system requirements. These include performing monthly system testing, completing an annual system self-assessment, establishing and maintaining standard configurations, and supporting quarterly and annual AHRQ FISMA reporting. These regulations require that responsibility be assigned for systems security, a systems security plan be developed, security controls be reviewed, and all changes to the security plans be approved by authorized managers in writing. MEPS next ATO is up for renewal in May of 2027.

The AHRQ-PSS Security Compliance Assessment and Authorization package was submitted to AHRQ on May 5, 2024 for ATO renewal. The plans and projects identified in the SSP directly relate to the NIST 800-53 Revision 5 security controls and are derived from staff interviews and system scans completed during the AHRQ-PSS Security Compliance Assessment and Authorization(SA&A) process in 2024. In conjunction with this process, the following materials were developed:

- System Security Plan;
- Risk Analysis;
- Configuration Management Plan;
- Contingency Plan;

- Incident Response Plan
- E-Authentication risk assessment
- Privacy Impact Assessment;
- Security Assessment Report (SAR)
- Plan of Action and Milestones (POAM) items.

Systems Test & Evaluations (ST&E) were conducted to verify the compliance with the security controls in the Systems Security Plan and with federal standards, Department of Health and Human Services (HHS) guidelines, AHRQ policies and guidelines, and current security industry and best-business practices. As part of the SA&A process, Westat has compiled the list of POAM items and continues to monitor and remediate identified security items, and report findings to AHRQ. Security policies, procedures, training materials, and other documents and artifacts associated with the SA&A requirements are being maintained and updated on an ongoing basis. As part of a recent HHS mandated initiative, Security Content Automation Protocol (SCAP)-compliant system configuration and vulnerability scan results for all servers containing MEPS data as well as POAM items for outstanding scan vulnerabilities are sent to AHRQ Security on a monthly basis.

Westat observes high standards of Automated Data Processing (ADP) and data security practices as a matter of standard operating procedure. Westat's approach to security consists of policies and procedures that are designed to maximize the following:

- Confidentiality – access to data and systems is restricted to authorized users only.
- Integrity – data and software content are correct and can be relied upon.
- Availability – data and systems can be used when required to the extent possible. When service interruptions do occur, they are of short duration and confidentiality and integrity will be maintained.

Westat assumes responsibility for the security of data in media including: electronic storage (e.g., tape, disk); hard-copy storage (e.g., paper); and transfer (e.g., FTP, broadband transmission, mail delivery). Efforts are directed to preventing all forms of data security violations, whether they could result from malfunction of the computer system, environmental hazards to the facility, or accidental or intentional misuse or misappropriation of the data or the system. Monitoring of security is achieved through carefully planned management practices, control procedures, and facility/equipment standards, which are discussed in the following sections.

Key aspects of the approach are summarized below.

- Procedural Rules
  - Establish rules of behavior concerning use of, security in, and acceptable levels of risk for each system. The rules are based on the needs of various users of the system. The security required by the rules is as stringent as necessary to provide adequate security for the study information. These include defining roles and responsibilities, consequences for not observing the rules, and appropriate limits

on interconnections to other systems. Incident response capabilities are established. The continuity of security practices and procedures are reviewed on an ongoing basis.

- Personnel Security
  - Establish employee security awareness and training program, and maintain lists of persons and their authorization privileges to computer passwords and systems.
  - Westat staff undergo an annual security awareness training and an annual human subjects awareness training. All project staff are required to take additional security training specific to the client agency. A list of trained individuals will be maintained and provided to the COR upon request, including staff with significant security responsibilities and role-based training courses completed
- Physical Security
  - Control access to facilities that process sensitive data, by the use of locks on doors and windows; secure the handling, labeling, and storage of sensitive data; dispose of or erase unneeded sensitive physical media;
  - Establish a fire emergency preparedness plan; use fire-rated walls, ceilings, and doors for construction of computer facilities; provide emergency hardware, marked exits, smoke/fire detection systems with alarms, fire suppression equipment, and waterproof covers to protect computers from water damage;
  - Establish an emergency power program; provide emergency power shutdown controls for computer equipment and air conditioning systems with protective covers to prevent accidental activation;
  - Westat limits physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protects the physical facility and support infrastructure for information systems; (iii) provides supporting utilities for information systems; (iv) protects information systems against environmental hazards; and (v) provides appropriate environmental controls in facilities containing information systems.
  - Maintain an inventory of all hardware and software; and
  - Destroy source documents as approved by AHRQ and other related waste material securely. The Westat Archive Tracking System (WATS) tracks the contents and status of boxes of archived materials.
  - System and Media Sanitization - Disposal will be done in accordance with NIST Special Publication 800-88, "Guidelines for Media Sanitization". Acceptable media sanitization methods commonly used at Westat include destruction and degaussing of magnetic media when the assets are physically retired, and multi-

pass overwriting on information system locations where the physical media will be re-used.

- Computer System Security
  - Separate the user and master modes of computer operations and install controls to prevent unauthorized access to the executive software system; protect operational status and subsequent restart integrity; and maintain complete and current documentation; and
  - Require and protect the secrecy of passwords and log-on codes; limit the number of unsuccessful log-on attempts; record occurrences of nonroutine activity; install an automatic lockout feature when a terminal is inactive; and establish automated audit trail capability.
  - Access to secure computer systems is password protected. All server and network data storage areas are protected by access privileges, which are assigned by the appropriate system administrator. Login passwords are encrypted and stored only in their encrypted form in protected files on each system. A non-displaying or non-printing feature prevents the password from appearing on the computer screen during the login process. The system automatically limits the number of unsuccessful attempts to log in, after which the account is disabled and must be reset by the system administrator. To ensure the confidentiality of passwords, users are required to change their network passwords every 60 days.
- Communications and Network Security
  - Implement secure data transmission procedures; and
  - Separate transmission of collected data (numerically encoded data) and the executable instrument (survey questionnaire) that relates numeric data value to substantive information.
- Cloud Security
  - Any cloud-based IT solution will be FedRAMP certified by a third party assessment organization (3PAO), and security assessment reports will be provided to the CO and COR for inclusion in the system security plan. Westat leverages cloud resources for both corporate and project needs when appropriate. Security of information in the cloud is a collaborative effort, with Cloud Service Provider (CSP) responsible for securing the cloud assets, and the Westat responsible for security of what is placed in the cloud. To ensure the CSP operates a secure environment, Westat only permits use of CSPs who have received a Federal Risk and Authorization Management Program, or FedRAMP, Authorization to Operate (ATO). Westat's standard security policies and requirements then apply to all information, assets, and systems placed in the cloud for which Westat is responsible.

In describing the data security procedures being implemented for the MEPS project, federal guidelines for security safeguard requirements are addressed as appropriate within sections of Chapter 1 of this plan. The sections in Chapter 1, in addition to this introductory section, are described below:

- Section 1.2 discusses risk assessment and risk management.
- Section 1.3 discusses personnel security. Sections specifically address hiring practices, staff reviews, security awareness and training, the separation of duties, and security officers.
- Section 1.4 discusses physical security. Sections discuss building security, physical media protection, and hard copy security.
- Section 1.5 discusses data processing security. This section specifically addresses computer operations, applications security, and communications security.
- Section 1.6 discusses contingency planning. Sections specifically address disaster recovery, including fire protection and power failures, file backup, file recovery, hardware backup and recovery, and communications backup.

In conducting the MEPS, Westat is responsible for developing and maintaining the field management systems, the computer assisted personal interviewing (CAPI) software, computer assisted video interviewing (CAVI) software, computer assisted data entry (CADE) systems, the scanning and verification of hard copy questionnaires, the editing of data and the development of analysis software, and maintaining the central database.

2. Risk Assessment and Management

The most valuable single asset of a data processing system is the data it produces. If the system does not protect the Confidentiality, Integrity and Availability of the data or its ability to produce that data, then the asset is at risk. At the organizational level, potential risks that threaten data security must be anticipated through an analysis of risk and appropriate procedures implemented to safeguard data systems. During the last ATO SA&A process in 2024, a formal risk analysis was developed and reviewed. This section summarizes the formal risk assessment, and the risk matrix is included in the Contingency Plan submitted with the required ATO documentation. Risk assessment occurs continually as systems are designed, maintained, and/or enhanced throughout the life cycle of the project.

2.1 Risk Assessment

The objective of risk assessment is, first, to identify vulnerabilities and potential threats to the security of data and computer application systems and, second, to evaluate safeguards that can provide the most cost effective protection against the identified threats and vulnerabilities. There are three major sources of risks that potentially threaten data assets, each discussed below:

- System malfunctions or failures;

- Environmental hazards; and
- Accidental or intentional misuse of the system or the data.

2.1.1 System Malfunctions or Failures

This source of risk includes those resulting from poor design, planning, testing, or maintenance of the operating system, application and system programs, communications systems, or their associated hardware. Faulty equipment can cause data to be lost or altered as it is being collected on laptop computers, transmitted to the home office, or stored in the database. Design flaws or "bugs" in the system programs, application software, or the database structure can potentially jeopardize the integrity of the data entered in the database or retrieved for analysis.

The best safeguards for preventing these potential threats from jeopardizing the data are thorough program testing, automatic backup procedures, and sound quality control procedures. Personnel training, supervision, and professional management practices can minimize risks due to operator error. Investing in high quality computer products and contract maintenance agreements for all equipment minimizes the risks due to malfunctions or failures.

2.1.2 Environmental Hazards

This source of risk includes threats from natural disasters such as fire and flood, as well as from insufficient environmental controls such as air conditioning, electrical outages, and noise in transmission lines. Computer equipment, tapes, and disks can potentially be damaged from exposure to heat, smoke, water, or debris. Power surges and electrical outages are a constant threat to computer operations. Maintaining temperature and humidity control is vital to proper computer functioning. Data transmissions are particularly vulnerable to interferences in transmission lines.

These risks are minimized by installing computer equipment in environmentally protected areas supported by a reserve power supply and routine backup procedures as currently implemented at Westat. Computer operations facilities have been constructed with specialized environmental controls, fire protection systems, an uninterruptible power supply and diesel-powered backup generators. File backups are made routinely and regularly. Tapes and disks are stored in fireproof vaults both on-site and off-site.

2.1.3 Accidental or Intentional Misuse of the System or the Data

This source of risk includes those associated with inadequate access controls to the facilities, systems, equipment, and data. This category also includes opportunities for entering erroneous or falsified data into the database; inadequate personnel supervision; broken, lost, or stolen laptop computers; and auditing procedures. Another source of intentional misuse of the system is computer viruses.

Inadequate access controls can potentially allow unauthorized entry into the computer system or facilities and even malicious destruction of data or equipment. Without adequate protective measures, hard-copy data collection materials can be lost or intercepted in the mail. Data entry errors, unintentional deletion of data, as well as inadequate supervision of data collection and data entry staff, can potentially reduce the integrity of the data. Inadequate auditing procedures can limit the ability to trace, identify, and correct problems as they are encountered.

Measures to prevent these occurrences include a user identification code and password system; thorough edit checks built into the data capture systems; automated audit trails; thorough personnel training, management, and supervision; reduction in the use of paper materials; secure mailing procedures; routine virus checks; and automated backup systems.

2.2 Risk Management

The best way to manage risk is to prevent those events that threaten data security from ever happening. In many cases, this can be achieved by implementing sound, verifiable information management practices and control procedures. But in some instances, even the best security management practices may only reduce the risk. Then, additional methods must be established for minimizing the damage caused by an occurrence of the risk and for the efficient recovery from it.

The recommended safeguard procedures outlined in Section 1.2.1 are fully implemented by Westat and its subcontractors throughout the HC. The major elements of our risk management program include:

- Personnel hiring, training, and management policies that maximize the professionalism and technical skills of all employees;
- Confidentiality agreements signed by all employees that ensure cooperation in protecting the confidentiality and security of data collected;
- A computer operations center that has controlled access, is protected from environmental threats, and has reserve power supplies;
- Secured work areas where confidential data and documents are held;
- Controlled access to computer terminals, accounts, network system, and files through user identification codes and passwords that are changed frequently;
- Protection against computer viruses by routinely running virus check software regularly and when any outside files are installed;
- Software development procedures that include thorough testing, built-in edit and consistency checks in all data capture systems;
- Automated audit trails and logs;
- Protected data transmissions and automatic backup files;
- Accurate inventory of all hardware and software; and
- Contingency planning and policies that include backup and recovery procedures for files, hardware, and transmitted data; procedures for handling cases residing on lost or stolen laptop PCs; and plans for disaster prevention and recovery including alternate Westat site data processing capability.

The details of implementing each element of our risk management program are presented throughout the remaining sections of this chapter.

3. Personnel Based Security

3.1 Personnel Security Policies

Qualified candidates for project-related positions or within the systems support areas are screened by key management staff and references are verified. Each Westat employee and contractor is instructed in Westat's data security polices, standards, and procedures by the employee/contractor's manager/supervisor. These policies are reviewed with staff on a periodic basis to maintain security awareness. Westat's management structure provides for separation of functions and responsibilities to limit any individual's access to and control of the data and the system.

All Westat employees and contractors are required to read and pledge compliance with a general code of conduct and assurance of confidentiality. A thorough understanding of this confidentiality agreement is required of all Westat staff. The confidentiality forms are electronically signed annually and delivered to AHRQ as one report for Field Staff and one report for Home Office Staff in April of each year.

In addition to signing a general assurance of confidentiality agreement, all home office staff, field staff, corporate staff who are responsible for the configuration of the MEPS infrastructure, data management, as well as any outside contractors assigned to the MEPS project are required to sign before being granted permission to access the MEPS project resources a copy of the MEPS confidentiality agreement, which addresses requirements for protecting the MEPS systems/data and penalties for violating the confidentiality of information collected for the Agency for Healthcare Research and Quality (AHRQ). Employees are required to read and sign the agreement annually (see Exhibit 1-1). Each April, reports are sent to AHRQ.

Exhibit 1-1. AHRQ affidavit for contractors

The Agency for Healthcare Research and Quality (AHRQ) collects and analyzes data for the purpose of carrying out policy research and quality analyses. The success of this aspect of the AHRQ program depends upon the voluntary cooperation of States, of establishments, and of individuals who provide the information required by Agency programs under an assurance that such information will be kept confidential and be used only for statistical purposes.

AHRQ operates under the restrictions of Section 903(c) of the Public Health Service Act which provides in summary that no information obtained in the course of its activities may be used for any purpose other than the purpose for which it was supplied, and that such information may not be published or released in a manner in which the establishment or person supplying the information or described in it is identifiable unless that establishment or individual has consented.

Unauthorized disclosure of confidential information is subject to penalty under Title IX of the Public Health Service Act, 42 U.S.C. 299, Section 924(d), which reads as follows: "Any person who violates Subsection (c) shall be subject to a civil monetary penalty of not more than $10,000 for each such violation involved. Such penalty shall be imposed and collected in the same manner as civil money penalties under Subsection (a) of Section 1128A of the Social Security Act are imposed and collected."

The laws excerpted below provide penalties for unauthorized disclosure of confidential information. Their full text is attached: **Section 513 of PL107-347:** "Whoever, being an officer, employee, or agent of an agency acquiring information for exclusively statistical purposes, having taken and subscribed the oath of office, or having sworn to observe the limitations imposed by Section 512, comes into possession of such information by reason of his or her being an officer, employee, or agent and, knowing that the disclosure of the specific information is prohibited under the provisions of this title, willfully discloses the information in any manner to a person or agency not entitled to receive it, shall be guilty of a **class E felony** and **imprisoned for not more than 5 years** or fined not more than **$250,000,** or both."

Unauthorized disclosure of confidential information is also punishable under **The Privacy Act of 1974, Subsection 552a(i)(l),** which reads as follows: "Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established there under, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it; **shall be guilty of a misdemeanor and fined not more than $5,000**."

It is highly important, therefore, that you understand your obligations regarding confidential information. You also agree not to link MEPS files that would permit the identification of the MEPS respondent unless the linkage is conducted under an approved project. Your signature below will indicate that you have carefully read and understood the above statements.

Typed/Printed Name	(Signature)	(Date)
Organization/Agency	WINS Number	

To ensure that data collected on this project are not available to anyone except authorized project personnel, a set of stringent confidentiality procedures are imposed on the field and telephone operations as well as on data processing.

- All employees sign an assurance of confidentiality.
- Employees are obliged to keep confidential all names and other personal data learned through the course of the data collection or incidentally.
- All field workers and telephone interviewers have been subjected to background checks.
- A field worker or telephone interviewer may not knowingly collect data on a study subject he or she knows personally.
- Survey data are kept locked when not in use. Access is limited to authorized personnel.
- The project director is responsible for ensuring that Westat personnel and subcontractors are in compliance with all security procedures.
- The project director ensures that survey practices adhere to the provisions of applicable contract provisions.

Data collection procedures, such as the assignment of study identification numbers to all subjects, are designed to guarantee confidentiality according to Federal regulations.

The day a staff member leaves Westat access cards are deactivated, and office keys are relinquished. Usernames and passwords are deactivated to ensure that the departing employee no longer has access to project directories or network drives, password protected software or any other computer systems that he/she had access to before. The departing staff member is also reminded that he/she has signed an assurance of confidentiality and what that means now that the staff member is departing. Field staff are required to return all computer equipment, IDs, and study materials prior to termination.

3.2 Security Awareness and Training

In addition to the security requirements specified in the confidentiality forms, security awareness and training is provided annually through a corporately developed program, project training sessions and specific instructions given to employees. As a part of the standard Westat security procedures, employees are told to keep the names of respondents, any opinions collected, and all respondent information strictly confidential and to prevent others from gaining access to confidential information in their possession. Employees are also told that, upon encountering a respondent or information pertaining to a respondent personally known to him or her, an employee is to terminate the data processing activity and contact a supervisor for instructions.

When a new hire or consultant begins a position specifically within the data processing division, the employee is informed about the company's data security policies, standards, and procedures by the employee's manager and receives security awareness training in conjunction with the new employee orientation. Before receiving their account assignments, new programmers and system

operators are instructed in the security policies, password systems, backup procedures, and audit trails established within various hardware and software configurations. All staff members receive a security badge with a photo ID and building access card. Staff are required to display the ID badge at all times while on the Westat campus. Staff without a valid ID badge must register as visitors upon entering any Westat facility. Home office staff are informed about specific documents that are considered confidential and the procedures for protecting these materials. Secure work areas for storing confidential materials are designated, and employees are instructed when and how doors are to be locked.

Field interviewers are given instructions during their training on specific measures established to protect the security and confidentiality of the data they collect. For example, the data are not to be disclosed to any unauthorized person outside the reporting unit (RU).The project supplies each field worker with a shredder to use for destroying materials with respondent identifiers. Most identifying information about an RU is stored in the computer so there is a limited amount of information in hard copy format. Procedures for mailing hard-copy data collection materials securely are specified, such as mailing via Federal Express. This service ensures timely and traceable delivery of the
hard-copy materials.

3.3 Personnel Implementation of Security Procedures

Data collection and processing duties are segregated into specific functional groups with clearly defined responsibilities and parameters. This separation of duties provides protection against staff members misusing the facilities by limiting their access and control to specific components. No group or individual can function independently of the others.

Within each group, staff members are assigned specific tasks for which they are responsible. Exclusive individual responsibility, however, can pose a danger to the stability and continuity of the facility. If an individual is moved from a key position without providing a suitable person to perform the task in his absence, the result could be a disruption of service. Therefore, staff members are cross-trained within each functional group so that no individual can become irreplaceable.

Periodic security audits are performed to review and monitor the implementation of security procedures. Each staff member has specific responsibilities for implementing security policies:

- The Project Director has overall responsibility for the security of the project and for coordination of the security administration team.

- Computer Operations Managers have responsibility for the integrity and reliability of the operating system and communications systems. Responsibility for the security of the operating system includes maintenance of disk libraries, hardware maintenance, control of user identification codes and passwords, backup systems, and contingency planning. Operations Managers supervise the operations staff and systems administrators to ensure that they comply with security standards and control access to the computer facilities and operating systems.

- Application Development Managers oversee the development and maintenance of the CAPI, CAVI and CADE program modules, survey management software, and analytical

software. Application development managers are also responsible for ensuring that programmers follow the programming and data security standards.

- Data Preparation Managers are responsible for all activities involved in the receipt, preparation, and handling of survey materials. They ensure that hard copy survey materials, including printouts from the database, are maintained in secure environments and that access to these documents is controlled.

- Data Entry Supervisors oversee the entry and verification of data through CADE and Teleform Scanning systems. They are responsible for ensuring that the operators conform to the data security standards. Security of hard copy materials must be ensured during the data entry process.

- Field Operations Administrators are responsible for field interviewer and field manager activities and for ensuring that the field staff follow the data security policies. The field operations administrators are responsible for protecting the confidentiality of the data collected and overseeing interviewer compliance with the confidentiality requirements of the Privacy Act.

- Building Security Managers are responsible for establishing and monitoring building security measures and building maintenance staff, including cleaning personnel.

4. Physical Security

4.1 Westat's Building Security

Facilities access control is a cooperative effort among staff members. Building security guards are the first line of defense. All staff wear visible photo ID badges at all times. Managers and supervisors oversee access security for areas within their domain. All employees are instructed to report any suspected security violation to their supervisor/manager. Video Surveillance cameras are situated in selected locations at Westat, and in the MEPS laptop processing and storage area to provide additional security. These cameras are on 24 hours a day, 7 days a week and can be monitored by Westat's security personnel.

Access to the Westat headquarters building is controlled before and after normal working hours and on weekends and holidays. Entrance to the building is restricted to authorized personnel through a key-card lock system. Westat's personnel department issues key-cards on a need-to-access basis and maintains the list of authorized key-card holders. MEPS staff members have keys so that they can lock their desks, filing cabinets and their office doors.

Within the Westat home office complex, special secured areas have been set up for specific data processing functions such as application development, data editing, and printing of confidential data. These areas are locked during non-business hours, and access is limited to authorized personnel only. Areas of special sensitivity are labeled as off-limits to all persons without special clearance, including cleaning personnel. Master keys are issued only to designated personnel and will open doors only in particular areas, with the "grandmaster" key, which only the building

manager has, being needed to open all doors. The managers of these areas are responsible for maintaining the lists of authorized personnel.

The Westat data center managed by Coresite is located in Reston, VA. Secure access restrictions are implemented to control data center access. Westat equipment is further protected by cage access restricted to Westat personnel. The data center maintains HVAC, electrical, Fire Suppression, Generator, UPS and monitors all environmental systems in real time.

The Westat headquarters building in Bethesda, MD is protected by an ADA compliant fire alarm system with visual devices, pre-recorded voice evacuation, public address, and two-way firefighter's communication. The building is fully sprinklered with a wet pipe system in office areas and a dry pipe system in the garage levels and loading docks. The building features fire-rated walls, ceilings and doors, and fire extinguishers and alarm pull stations are place throughout. The building is equipped with three emergency generators that will provide power for emergency lights in the event of a power failure.

More detailed information on the MEPS System Security can be found in the AHRQ-PSS HVA System Security Plan, a component of the Security Assessment and Authorization package developed in November, 2011.

4.2 Security of Hard Copy Materials and Physical Media

Access to all study data is limited to project staff. A list of authorized project staff members is maintained by the project director or person designated by the director.

All project personnel are instructed in the importance of protecting data confidentiality and are aware of what constitutes sensitive data. Therefore, project staff members can easily recognize materials which contain confidential data.

4.2.1 Security of Hard Copy Material

Westat personnel are instructed in the importance of protecting data confidentiality. Data in hard copy format are kept in locked cabinets or areas when not in use. Access restriction signs are posted at the entrances to secured data processing areas. Likewise, system-generated output containing confidential data is also stored in locked areas. Receipt control systems are designed to track the location of paper documents and, thus, detect missing ones. Self-administered questionnaires requiring confidential handling and other required supporting documentation are stored in a limited access facility. Staff working with confidential receipt control, coding, editing, or data entry have access only to the materials they are currently processing.

During home office processing, the movement of hard copy through the various processing steps is continually audited by the survey management system. The system provides management reports by location so that processing supervisors can track the documents. Locked repositories are used to store survey authorization forms and other sensitive hard-copy materials. System generated data are identified by ID, not by a respondent's name.

When hard-copy material is mailed, it is sent via Federal Express and personal identifiers are minimized to the extent possible. Federal Express has been chosen for its reliability and ability to locate mail if it does not arrive at its destination on time. Whenever a package with hard copy materials containing confidential information is shipped, the person sending the package must

email the recipient and notify him/her of the expected date and time of arrival of the package as well as the tracking number on the package label. Packages that do not arrive at the expected date and time are traced through the Federal Express tracking system.

Hard copy documents with confidential information are shredded as soon as it is determined that they are no longer needed in support of project work.

If hard copy material with personally identifying information is lost key project staff at AHRQ, the AHRQ Information Security and Privacy Team, and Westat home office staff are notified within one hour through an interactive voice response (IVR) system. In addition, Westat's Institutional Review Board (IRB) is notified. Details of the detection and notification system are provided in the Incident Response Plan for the MEPS enclave system.

Recently, many hard-copy materials used by the interviewers and supervisors have been converted to reports available in the BFOS system. This has allowed for a significant reduction in PII information on media outside of the laptop.

4.2.2 Procedures for the Distribution of Data Files

Westat uses secure FTP sites for the distribution of data files to AHRQ and other sub-contractors. Files for a single delivery are each encrypted using Securezip, a 140-2 validated encryption software and zipped into one delivery file which is password protected using the standard Westat convention. All laptops or other portable devices employ FIPS 140-2 compliant Whole Disk Encryption (WDE) (currently Bitlocker), in addition to session-level encryption (TLS) for study-related data transmission. All server-based storage is backed up to a secure FedRAMP authorized Cloud Service Provider (CSP) on a daily basis.

4.2.3 Procedures for Destruction of Source Documents and Other Contract-Related Waste Material

Project documentation is kept for the duration of the agreed-upon retention period. The storage of the materials is handled by an external firm. This firm is reputable and bonded. When the retention period has expired, the owner of the documentation is contacted to determine if the contents should continue to be retained for some reason or if the boxes of documentation should be destroyed. If the owner wants to continue to retain the information, the retention date on the box is modified. If the materials are no longer needed, they are destroyed (shredded or burned). Locked containers are located throughout the MEPS working area for discarded materials; these are shredded bi-weekly on site by a contracted external company.

When electronic storage media are no longer required, they are either erased before being reused or disposed of in such a way as to ensure the destruction of data they contain. In addition, protected network files and databases are backed up and archived.

4.2.4 Security of Physical Media

Westat provides an on-site fire-resistant cabinet for storing production disks and CD-ROMs and disks until they are transferred offsite for long term storage. The room is locked at all times and access is restricted to authorized project staff.

Project media (tapes, CDs, DVDs, USBs, etc.) that contain data, but are no longer serviceable, are destroyed by degaussing, low-level formatting, physical destruction, or other industry-approved destructive methods. The method selected is done in accordance with NIST Special Publication 800-88, "Guidelines for Media Sanitization" and is dependent on the media type and sensitivity of the information which it holds. Project media that can be reused have low-level reformatting or other industry-approved destructive methods for destroying any data performed on the media before being released back into use.

For paper records that need to be destroyed, Westat has several methods of destruction available for project staff. The following are located throughout Westat office spaces:

- Stand-alone paper shredders
- Non-secure paper recycling containers for NON-SENSITIVE documents
- Secure paper recycling containers for SENSITIVE documents

4.3 Security of Devices

The security systems and procedures implemented for laptops and iPhones are designed to protect the data from accidental alteration and unauthorized disclosure.

Laptop PCs and iPhones are assigned to specific interviewers and field supervisors at the beginning of each data collection period. The CAPI and CAVI system controls the user IDs and passwords so that if a device must be replaced due to non-operating parts or if the device is lost or stolen, the CAPI and CAVI system can reassign data access rights to another device. Thus, if an unauthorized user tried to access software or data after powering-up the project-assigned devices, the CAPI and CAVI menu would require a user ID and password.

Procedural security measures have also been implemented on HC to assure the confidentiality of data on laptops. These include:

1. **Interviewer Procedures.** Interviewers are instructed not to keep information about passwords with the computer. Interviewers are trained in secure methods for storing laptops and traveling with laptops to minimize the risk of losing laptop computers. MEPS interviewers can report the loss of a computer 24 hours a day, 7 days a week, to initiate action from the home office through the IVR system.

2. **Systems Procedures.** When a laptop is reported as missing, any incoming or outgoing transmissions to that laptop are blocked. Any e-mail directory or file transfer privileges are removed to prevent any unauthorized transmission of messages or data. Passwords regularly expire according to best-practice security policies.

3. **Administrative Procedures.** Whenever a laptop is reported as missing, either Westat or the interviewer involved files a police report and initiates whatever action is possible to attempt to recover the equipment as soon as possible. AHRQ is also immediately notified of the loss and the Westat IRB is informed.

If a “missing” laptop must be replaced in the field, the following procedures are used:

- The interviewer and/or field supervisor notifies the home office as soon as possible about the broken or missing computer.
- The home office computer staff removes the node (the missing computer) from the user list on the transmission server.
- Data base records for all cases allocated to that interviewer are locked and immediately reviewed by the home office staff. This is done in consultation with the interviewer and supervisor.

When the interviewers are using the laptop computers in the respondent’s home or later when they are transmitting data back to the home office, they are instructed to use the AC power adapter whenever possible. Spare batteries are provided with each assigned laptop in locations without access to AC power to ensure the continuity of the interviewing process.

5. Data Processing Security

Sound programming practices are vital to the security of a system. Toward that end, the information systems departments have established procedural methods for application development and maintenance providing control, verification, and documentation within the programming environment.

Only computer operations managers have the privilege to bypass user mode restrictions in accessing the system to perform general system maintenance activities. All other users are restricted to user mode and a subset of operating system commands and functions.

Computer systems are monitored by the operations staff during regular business hours as well as evenings and weekends. In the unlikely event of a system failure, Westat maintains field service contracts with equipment vendors. Westat also operates an on-site repair facility for various technical equipment and maintains an inventory of replacement servers, workstations, and other key components.

Purchase, installation, and maintenance of PC hardware and software are under the control of Westat’s PC Technical Services group. Personal computers are registered with the group, and repairs and component replacements are done on site. To avoid invasion of the Westat PCs by foreign viruses, Westat primarily installs software purchased directly from the manufacturer. Public domain software may also be made available to Westat. This software is tested by using a computer program designed to detect viruses. The software is tested on a PC with an expendable hard disk, and the test is run through numerous iterations over a period of time since the onset of a virus may be time delayed. This same detection service is provided to all Westat users who obtain software from sources other than Westat. This software is run continually while the PC is in use. Network drives are backed up daily, and only approved software is loaded on system drives.

In addition, network and system drives are scanned daily and the software is configured to execute upon new/modified files in real time. The virus scanning software is updated and distributed to

network servers and workstations in an automated way on a regular basis to ensure that currently reported viruses will be detected.

5.1 Account Protection

All files are created and stored within accounts. These accounts are maintained by computer operations managers and are associated with specific processing functions, such as program development and receipt operations. Accounts are used to collect charge data, catalog files, and provide a means of access control. Accounts are divided into three types:

- **Development Accounts.** Development accounts are assigned to individual programmers for creating and modifying programs. Development accounts do not store or access production data.

- **Test Accounts.** When a program is ready to be tested, it is moved from the programmer's development account into the test account. All program testing is performed from the test account and all test data are stored in the test account. Because the testing environment must be tightly controlled to obtain accurate results, these accounts are restricted to personnel involved in testing.

- **Production Accounts.** After testing is completed, the program is moved from the test account into the production account. All production processing is performed through this account. All production data files reside in production accounts.

5.1.1 Password Protection

Access to all corporate computer systems is password protected. All host, server, and network accounts are protected by passwords and disk access privileges are assigned by the system administrator. Passwords are initialized by security management, then encrypted and stored in protected files. The password encryption cannot be removed. A non-displaying/non-printing feature prevents the password from appearing on the screen during the logon process. The system automatically limits the number of unsuccessful attempts to logon after which the account is disabled and must be reset by the system administrator. To ensure the confidentiality of passwords, users are required to change their passwords every 60 days. Passwords must be a minimum length of 12, meet certain character rules and standards, and cannot be reused. Accounts that have not been used in over 60 days are identified for deletion.

If the password is not changed after computer prompts at the end of 60 days the users are allowed to log on one last time ("grace" logon). Then all users will be locked out and unable to log on, and computer operations management must be contacted to obtain a new password. When passwords are being changed, the system rejects any new password which does not meet the minimum password length and criteria established by computer operations management. The system also keeps a list of previously used passwords for each user and rejects a password change which attempts to use any of the previous ten passwords. Thus, the system assures that there is an actual password rollover rather than just a refreshing of an old password.

The system automatically limits the time allowed for the user to type in the correct username and password. If the user does not enter each of these in less than 30 seconds from the time the prompt appears, the session is ended. Incorrectly entered passwords on laptops are limited to three attempts and then the user is forced to wait for 15 minutes before a password may be re-entered.

Incorrectly entered passwords on desktops are limited to three attempts and then the user must contact corporate security staff to gain access. Furthermore, computer operations management may impose stricter break-in evasion controls for selected accounts containing sensitive files. If the number of unsuccessful attempts to access one of these accounts exceeds the limit, access is denied for a period of time.

5.1.2 File Protection

Access Control Lists (ACLs) provide an added level of access protection at the file level. This higher level of control can restrict access to specific files within an account which may contain confidential data or critical procedures while allowing wider access to less sensitive portions of the account. Computer operations management creates entries to the ACL to define which users or system programmers may have access to the file and which access rights each user will be granted. When users enter their passwords, the system first searches the ACL. If a match is found, the user is allowed or denied access according to the access rights associated with the ACL entry.

5.1.3 Network Systems

Access to the LANs is password and time of day restricted. Individual files are protected by granting access rights only to authorized users. Data on the LANs are further protected by scheduled backups. (See Section 1.6.1, File Backup and Recovery.)

Westat's network, Wesnet, provides three levels of access protection: network passwords, directory and file rights assigned to work groups and individuals, and attributes assigned to directories and files. When an employee registers for Wesnet, he or she is given a network account which specifies the employee's user name and a Wesnet password which the employee changes immediately to a unique word known only to the employee. The account is registered on the employee's home server, and the employee can use network services on any server on which he or she has an account. Thus, an employee has only a minimal use of services on any server on which he or she does not have an account.

Rights assigned to Westat work groups and individual employees protect files in network directories from damage, deletion, or unauthorized access. MEPS security managers (computer operations managers) assign employees the rights they need to the work group directories they use. These rights (read, write, create subdirectories and files, erase directory, modify directory, and scan for files) control which network directories, subdirectories, and files employees can access and what they can do in each.

Wesnet also secures files in network directories from data corruption and loss through backup procedures. Wesnet files are backed up nightly and in the same way that the Wesnet servers are backed up. (See Section 1.6.1, File Backup and Recovery.) The primary purpose of this backup is to protect the network from catastrophes such as the failure of a network disk. In an emergency, the network administrator can retrieve network files from the backups. This takes from two hours to one working day depending on whether the backup has been sent off-site for storage. Access to these backups is restricted, and Wesnet does not allow direct user access to system backups.

Employees are instructed to store all files in designated network directories so that they are backed up and secured as part of the corporate backup activity. Access to such files is restricted to members of the specified work group.

5.1.4 Operations Auditing

The Active Directory server records system activities and produces a variety of accounting logs. This utility offers computer operations management a versatile tool for monitoring system activity. It can provide an accounting of system activity for a given time period. For instance, by activating specific utility parameters, computer operations management can print a listing of all unsuccessful attempts to log on from a particular workstation during a certain period of time or can display all successful attempts to log on.

The system also provides a security alarm feature that can be used to monitor selected types of events at the file and account levels. By setting audit alarms, the system can audit a wide range of user activities including the following: break-in attempts and failures to log on, successful logging on, and volume mounts and dismounts.

Database management systems have extensive and robust security features. Regardless of the implementation platform, typically, we require personal accounts for all users, so database activity can be traced to individuals who have logged on using the password specific to that account. Accounts are assigned privileges based on the functions of the user within the application. Resource privileges and data definition privileges are restricted to accounts for programming staff. Database administration accounts are assigned only to a few trained and authorized senior staff. Passwords on critical accounts are rotated periodically. Generally, system auditing is implemented for commands related to data definition, security administration, and logon failures.

Dynamic backups are implemented, if needed. Regularly scheduled database backup procedures are coordinated with system backup procedures to achieve the highest level of protection and the minimal disruption of normal activities.

5.2 Applications Security

Application systems are designed to employ programming techniques in which the application is broken down into small components or modules, each performing a specific function and called by a controlling program. Beyond the obvious benefits to system development management and problem diagnosis, this type of program construction provides these additional security benefits:

- Because programming responsibilities for the application are divided among several different programmers, the risk of any one programmer manipulating the code to violate data security is minimized.
- Because the size of each module is small, it is much easier to detect faults within the coding which could compromise the integrity of the data.
- During system maintenance a problem occurring within a given module can be corrected without exposing the entire application system to risk.

5.2.1 Software Development Procedures

An application program is typically divided into several modules. Before an application module is assigned to a programmer, **systems staff** reviews each questionnaire to identify required inputs, range and consistency checks, condition logic, skip patterns, and subroutines.

All application programs and program modifications are thoroughly tested before they are implemented.

All programs are controlled and catalogued at the account level. After a program has been thoroughly tested, a designated member of application development management compiles the program from the test account to the appropriate production account and logs the action by program name, version number, and date of creation. The program is then protected by the access control rules set up for that account. As the program is compiled into the production account, a copy of the source code is added to a parallel production source account.

Production source programs are stored in production accounts with "read only" access, and within those accounts the source code is managed using version control software. When a production program requires modification, the programmer must "check out" the source code to a development account. After the program changes have been completed, the source code is checked back in with required documentation, and the program will follow the same testing and implementation procedures described above.

When a modified application is placed in production, a copy of the new version is immediately transmitted to all facilities running that application so that all sites maintain parallel systems.

5.2.2 Documentation

Westat maintains full documentation in order to have a record of all procedures, programs, decisions, and changes. In this way the information is available to all project staff, and the loss of any particular staff member will not result in the irremediable loss of knowledge to the project. The most important documentation for this purpose is the following:

- **Design Specification.** Detailed specifications for the CAPI instruments are prepared prior to the initiation of programming. These specifications are archived for each Panel and Round of MEPS HC.

- **Testing.** All problems encountered during systems or operations level testing are recorded. The problem documentation is then used to correct the program and is kept with the original design specifications. Also, transaction audit trails are produced to monitor performance and to detect possible sources of error.

- **Implementation.** Printouts of production source code, screen layouts, and data dictionaries are generated as part of the implementation procedure. Program hierarchy diagrams are created to support this documentation.

The production log which is controlled by program management serves as a permanent record of implementation activity. Production account directories may be accessed by authorized application development managers to obtain a complete list of programs catalogued in the production accounts.

- **Program Maintenance.** An on-line problem reporting system has been developed to document and monitor problems encountered during processing. The user enters the problem on a special screen to create a record in the problem management file. Application development management reviews each problem record to determine if program modifications are necessary.

If so, modification specifications are prepared and assigned to a programmer. If not, the problem is fielded to the responsible management team for resolution. Application development management updates the problem record to reflect the disposition of the problem and, when the problem is solved, the actions taken to correct the problem. The problem reporting system offers a means of tracking the age, disposition, and status of problems so that they can be resolved quickly with minimal disruption of production activities. During modification coding, the programmer inserts comments into the program to document all changes made to the original version.

5.2.3 Database Design

Databases are designed to segregate personal identifiers from data. Personal identification information, such as names, are stored in a separate segment of the database and are represented in other segments by unique IDs that do not represent any specific individual characteristics.

5.2.4 Audit Trails and Logs

Westat's audit trail utility creates a complete record of every computer-assisted interviewing session. During testing, this allows programmers or data preparation personnel to ascertain whether particular anomalies in the test data are the result of keying error or problems in the program that require fixing.

Westat also keeps a log of all changes made to the data in its transaction journal. This helps to prevent data from being corrupted by incorrect updates. By looking at the transaction journal, a data preparation staff member can immediately see if a problem in the data is the result of a previous update that should not have been made.

5.3 Westat Field Operation System (FOS)

The Westat Field Operation System (FOS) is a corporate system that provides a ready and standardized management system framework within a proven and secure computing environment referred to as FOS Zone and Web Zone. These environments are used for field projects conducted by Westat. The system was adapted and augmented as needed to meet specialized needs of the MEPS project including the multi-panel design.

5.4 Home Office Systems

This includes the servers, communication and network infrastructure, and other devices that allow field staff to connect to the Westat home office facility and support centralized services such as the hosting of the web-based BFOS application, data transfer, and e-mail. The Home Office Systems include the following components and services:

- **Broadband internet connectivity**.
- **Web servers**
- **Databases**.
- **Data transfer**.

- **E-Mail**.
- **Data encryption**.
- **Box**.

5.5 Field Laptops

The MEPS FOS laptop will be configured with the following components:

- **Model** – HP EliteBook 840 G8 Notebook.
- **Operating system –** Windows 11.
- **Web browser –** Edge Chromium.
- **File transfer –** the file transfer client software is installed on the laptop.
- **Data encryption –** the laptop hard drives are encrypted using whole-disk encryption software.
- **Virus scanning –** virus scanning software is installed on all field laptops and configured to scan the hard drive when the laptop is powered on and when new data are written to the laptop.
- **FOS application –** the laptop resident portion.

5.6 Special Security Considerations

Security is a key consideration in the configuration and management of the FOS infrastructure both at the home office and in the field. The security features of FOS are intended to address the following concerns:

- Field data are securely stored to protect confidentiality and cannot be accessed or changed except by authorized individuals using designated systems. Data are also protected against accidental damage or loss.
- The operation of the system is reliable, the various technical services can be accessed by field staff when needed, and the system performs adequately.

Security is implemented in the FOS infrastructure through the use of the following tools, techniques, and practices:

- The central FOS platforms are installed in Westat's secure and controlled computer facility and benefit from the general technology planning and investments made by the company. This includes the operation of redundant Westat computer centers with controlled environments, a secure physical facility, redundant platforms, procedures to guarantee the security of platforms and data, and trained systems support staff.

- The FOS Infrastructure is installed on a sub-network within Westat and is isolated from other portions of the Westat network by a firewall. As a result, access to field platforms and data is not exposed to general Westat network traffic but is limited to those users that are involved in field operations support.

- Laptop security is provided by Symantec Endpoint Security, which protects the laptop against malware including all viruses.

- Field supervisors and field interviewers connect to FOS using broadband internet-based connectivity. This communication system provides actively-managed authentication and security policies. Users log into a local account for laptop access and authenticate to connect to Westat resources for which they are authorized by the home office. Users are required to change their passwords regularly and to use passwords of acceptable strength. The system has laptop-based security features that include anti-malware, firewall, intrusion detection, and the ability to control applications and field devices (such as CD-ROM drives and USB ports). Data encryption protects the entire laptop hard drive and protects individual files during transmission.

- Encryption technology is used to protect the confidentiality of data from unauthorized access. Both management and interview data are stored in an encrypted form on the laptop when it is not in use. Data are also encrypted during transmission to the home office. The connection to FOS web sites is also encrypted through the use of Secure Socket Layer (SSL).

- Commercial virus protection software is installed on laptops and home office platforms. All data are scanned for viruses before being written to any FOS platform.

- Data backups and transaction logs are maintained at numerous points within the data collection, transmission, and storage process. These backups can be used to restore or reconstruct data in the event of a platform failure or accidental data loss.

- The FOS platforms and applications are monitored through multiple automated monitoring systems. When problems are detected, support staff are alerted immediately.

Technical support to the FOS infrastructure is available as needed to meet project requirements.

5.7 Operational Support

Various corporate support functions are in place to support the operation of the FOS systems including:

- **FOS Application technical support –** the FOS application team provides technical assistance for initial planning when project requirements are mapped onto the standard BFOS field model, identifying and planning of custom changes to the BFOS databases or applications, understanding and working with the various technologies used by the BFOS application, and installing and testing the BFOS application.

- **FOS Infrastructure support –** FOS home office platforms and support infrastructure are managed and monitored by Westat corporate systems staff. This support includes daily data backups, resource and performance monitoring, operating system patches and upgrades, hardware maintenance, and problem resolution.

- **FOS Laptop configuration support –** corporate staff also assist the project in defining the appropriate laptop configuration for the field project. This includes certifying that the laptop hardware is compatible with the FOS system, insuring that the various components have been installed and configured in a secure and appropriate fashion, testing the operation of the laptop, and assisting the project in producing the number of final laptops required for the field staff.

6. Contingency Planning

Recognizing the need to insure continuity of data processing services and security regardless of circumstances, Westat has developed contingency plans for the MEPS project to establish procedures and systems for disaster recovery. The safeguards presented below have been developed to address potential security threats to data and data processing systems due to damaged or lost files, hardware failure, disruption in communications, or environmental disaster such as flood, fire, or power loss.

Our contingency plans include procedures to ensure continuity of data processing services at four levels. The first is file backup and recovery procedures for both data files and software files. The second level of contingency planning is procedures for hardware backup and recovery. The third level establishes communications backup and recovery procedures. Fourth, plans for disaster prevention and recovery establish emergency preparedness in the event of long-term loss of service due to damage to data processing facilities.

6.1 File Backup and Recovery

Westat file, database and application servers are backed up every day to a local, onsite backup appliance. Since electronic information is a valuable asset, several steps are taken to prevent the loss or corruption of data in case of equipment or facility failure. First, users are instructed to store all data files on network server directories rather than local PC hard disk drives. Second, Westat's Computer Operations staff back up all server-based storage to an onsite encrypted backup repository. After the completion of each backup, the data is also securely copied to a FedRAMP compliant cloud storage provider where it is retained for a minimum of 90 days. The daily backup data is retained locally for ease of access for a period of 28 days.

6.2 Hardware Backup and Recovery

Computer hardware used to support the MEPS project include laptop computers and iPhones for field data collection, local area networks at the home offices, and Wesnet servers. Backup and recovery procedures for this equipment must consider power supply and protection against equipment failure.

The power supply for Wesnet equipment at the Westat home office is supported by uninterruptible power supply systems (UPS) to minimize disruption due to power shutdowns. The UPS constantly filters and monitors the power supply. If the system senses a power problem, the backup battery supply takes over to maintain a steady power supply for network servers and Wesnet servers. In the event of an extended utility power failure, a separate diesel-powered standby generator provides continuous power for up to 5 days without refueling.

The network file server which stores the project-related files can quickly be replaced with another network server. There are numerous file servers on the Wesnet LAN and exactly the same software is loaded on all of these servers. Thus, users of a failed server can log onto another server in order to use network software with data on their local hard drive. Spare servers with the standard network software are available so that a fully configured server can replace a server down due to hardware problems. Replacement of an existing server with spare equipment can be accomplished in a little over one hour.

Westat has a formal disaster recovery plan to be used in the event of a significant failure of regular computing services due to fire, flood, long term power outage, or other events that have a major impact on systems operations. The plan identifies the primary and backup members of the disaster recovery assessment team and the functional systems area for which each person is responsible. If an event occurs that requires the attention of the team, all appropriate members convene to begin an assessment of the situation for their respective area and prepare an estimate of the time and level of effort required to restore operations. Restoration efforts are directed by the team leader, who coordinates these activities with other senior corporate managers.

Westat has field service contracts with computer service vendors for the Wesnet server disks. If there is a problem, the service vendor will respond within 2 to 4 hours to fix or replace the faulty component.

Westat also maintains an on-site repair facility and has a supply of spare equipment which can be shipped to any destination within 24 hours. For the MEPS survey, the laptop vendor will supply extra computers when necessary at specified locations.

Spare equipment is stored for use in most emergency situations. If spare equipment is not available, service contracts with outside vendors are maintained. A failed file server is usually operational in four hours or less. Procedures for properly shutting down equipment to prevent data loss or damage are made available to the appropriate personnel.

6.3 Disaster Prevention and Recovery

Westat has a formal disaster recovery plan to be used in the event of a significant failure of regular computing services due to fire, flood, long term power outage, or other events that have a major impact on systems operations. The plan identifies the primary and backup members of the disaster recovery assessment team and the functional systems area for which each person is responsible. If an event occurs that requires the attention of the team, all appropriate members convene to begin an assessment of the situation for their respective area and prepare an estimate of the time and level of effort required to restore operations. Restoration efforts are directed by the team leader, who coordinates these activities with other senior corporate managers.