Attachment 6: Abt SRBI, Inc. Systems Security Plan

Abt SRBI, Inc.

Systems Security Plan (SSP)

Version 3.2

March 9, 2015

THIS PAGE INTENTIONALLY LEFT BLANK

Abt SRBI
SYSTEM SECURITY PLAN
CHANGE INFORMATION PAGE

Issue	Date	Author	Pages Affected	Description
2.0	January, 17 2012	Dwight Feanny	All	Initial Version
2.1	September 10, 2013	Jim Harless	All	Version update
3.0	June 5, 2014	Jim Harless	All	Version Update
3.1	August 14, 2014	Jim Harless	All	Version Update
3.2	March 9, 2015	Jim Harless	All	Version Update

THIS PAGE INTENTIONALLY LEFT BLANK

Abt SRBI
SYSTEM SECURITY PLAN REVIEW/APPROVAL SHEET

Name:	Signature	Date

Name:	Signature	Date

Name:	Signature	Date

Name:	Signature	Date

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

Executive Summary

This Information Technology System Security Plan (SSP) describes the policies, procedures and controls by which Abt SRBI Inc. complies with its clients' Information Technology System Security requirements, and protects client data. This plan was developed in accordance with the standards put forth in the National Institute of Standards and Technology (NIST) Special Publications *800-18 revision 1, Guide for Developing Security Plans for Information Technology Systems, 800-53 revision 3, Security and Privacy Controls for Federal Information Systems and Organizations, 800-12, An Introduction to Computer Security: The NIST Handbook, and 800-14, Generally Accepted Principals and Practices for Securing Information Technology Systems.*

Abt SRBI operates a secure IT environment that supports the work it conducts for its government, Universities, non-profits businesses, and industry clients. The IT environment consists of a sophisticated Company network; connections to the Internet, including a secure, encrypted virtual private network (VPN); PC hardware and software; tape and disk backup; and data center hardware and software. A wide variety of commercial-off-the-shelf software (COTS) is available to provide document building and print services; office automation services; Internet services; statistical analysis; and network communications. In addition, the environment includes hardware and software used to support large-scale surveys, using a variety of data collection technologies.

Abt SRBI security methodologies include physical access control; logical control of access to the IT environment as a whole; specific authorization and logical control of access rights to data and programs, based upon specific need for access; extensive network and Internet security controls; management and operational controls; and monitoring.

The Abt SRBI IT environment is highly secure, and the procedures used within the Company have proven to be effective in ensuring the privacy and confidentiality of information. Nevertheless, security evaluation, risk assessment and improvements are a continuous process, as we seek to stay ahead of the growing threats to data security, and address our clients' concern for IT security, privacy, confidentiality, integrity, authenticity and accessibility.

1. Information System Name

Abt SRBI General Support System (GSS)

2. Information System Security Categorization

The GSS is categorized as a ***moderate-impact*** system per the guidelines contained in FIPS 199.

LOW	MODERATE	HIGH
	X	

3. Information System Owner

Abt SRBI, Inc.
275 Seventh Ave, Suite 2700
New York, NY 10001
Phone: 212-779-7700

4. Authorizing Official

The Senior Vice President of Information Technology has overall responsibility for Abt SRBI's Information Security Program

5. Designated Contacts

Table 5-1: Designated Contact Information

Organization	Point of Contact
Abt SRBI	**Dwight Feanny** Senior Vice President of Information Technology Abt SRBI 185 Monmouth Parkway, Suite B4 West Long Branch, NJ 07764 Phone: (732) 728-7100 Fax: (732) 728-1602
Abt SRBI	**Jim Harless** Information Security and Data Privacy Manager Abt SRBI 8405 Colesville Rd, Suite 300 Silver Spring, MD 20910 Phone: (301) 628-5505 ext 15505
Abt SRBI	**Steve Bibbo** Director, IT Services Abt SRBI 185 Route 36, Suite B4 West Long Branch, NJ 07764 Phone: (732) 403-2523 Mobile: (609) 276-7917

6. Assignment of Security Responsibility

The individual listed below have been assigned the function of the Local Security Officer (LSO) for SRBI's GSS. The LSO is also the primary contact for the GSS on all security and FISMA compliance procedures.

Table 6-1: Security Contact Information

Organization	Point of Contact
Abt SRBI	**Jim Harless** Information Security and Data Privacy Manager Abt SRBI 8405 Colesville Rd, Suite 300 Silver Spring, MD 20910 Phone: (301) 628-5505 ext 15505

7. Information System Operational Status

The Abt SRBI General Support System (GSS) is currently operational.

Operational	Under Development	Major Modification
X		

8. General System Description and Purpose

The Abt SRBI IT Environment provides the technologies used by Abt SRBI staff to perform their business and client service functions. It includes the company network environment; PC's and laptops; office automation software; hardware and software used for data management and statistical analysis; and hardware and software used to support large-scale surveys. These are described in greater detail in the following sections.

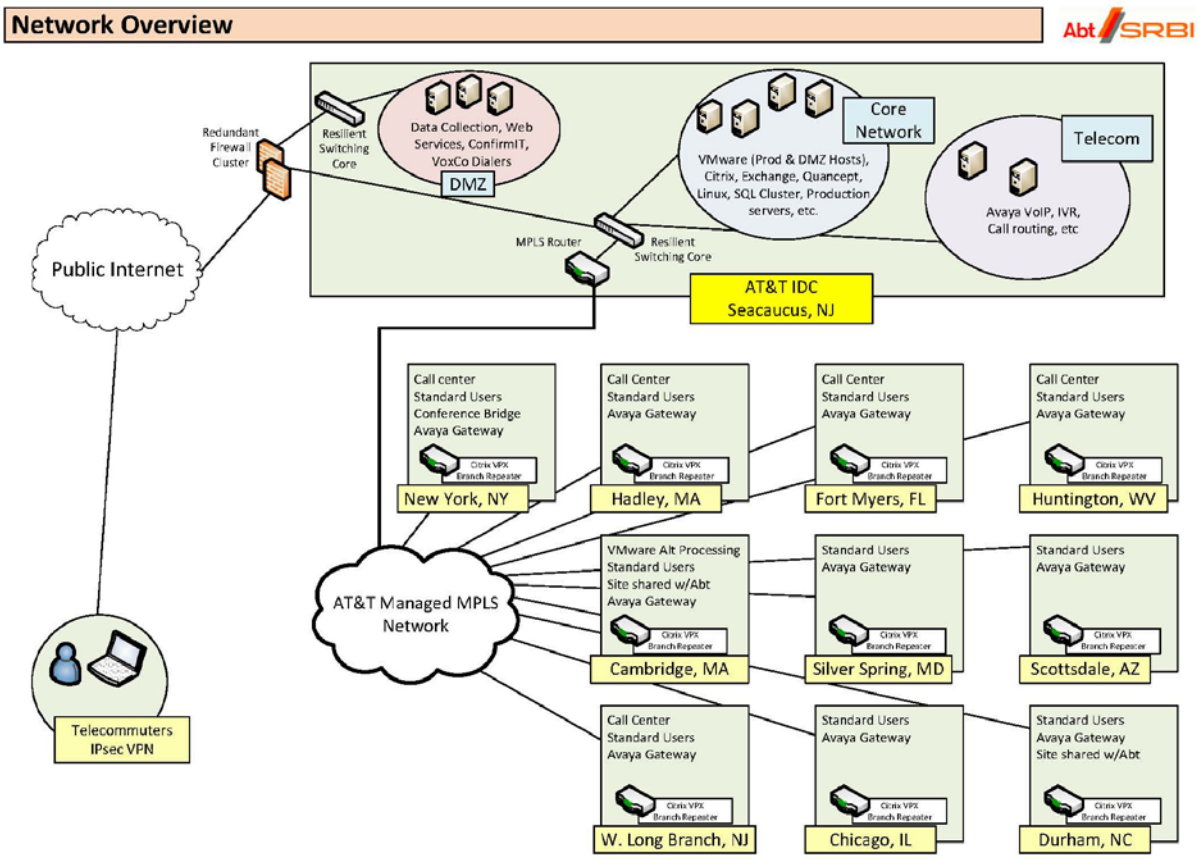
The Abt SRBI IT environment includes a wide variety of commercial off-the-shelf (COTS) applications used to support office automation, Internet services, statistical analysis and survey requirements.

9. System Environment

Abt SRBI supports local area networks (LANs) in all SRBI offices. This switched- Ethernet based LANs are interconnected by either a private wide area network (WAN) based on AT&T's dedicated MPLS technology; a point-to-point T1 leased lines, or an IPSEC VPN tunnel. Our Internet connections are protected by Sonicwall firewalls.

The Abt SRBI GSS infrastructure consists of communication devices, firewalls, and servers that are physically housed in a co-location in Secaucus, NJ. Administrator support will be located in various Abt SRBI offices throughout the country. GSS will be accessible to Interviewers and Administrative support via IPSEC VPN tunnels using private Multi-protocol Label Switching (MPLS) mechanisms from pre-configured client workstations (**Figure 9-1**).

Figure 9-1: GSS Infrastructure



The above-listed servers, PCs and applications operate within the Abt SRBI network environment. Access to Abt SRBI network and systems are limited to Abt SRBI employees and, where appropriate, designated consultants and subcontractors. Consultant and subcontractor use of Abt SRBI systems is subject to all Abt SRBI IT policies, procedures and security plans.

Abt SRBI uses a dedicated AT&T MPLS wide-area network (WAN) to provide data communications among its offices. In addition to the Company WAN, Abt SRBI maintains leased-line data communication links to the Internet in most of its offices. Each of these connections is protected by a Sonicwall firewall that controls access to the LANs, WAN, and DMZ. Encrypted connections across the Internet between sites are supported using Sonicwalls Virtual Private Network (VPN) facility. Sonicwall uses 256 bit AES encryption to communicate between firewalls. This functionality is used as a backup to the WAN in the event of a service outage.

Abt SRBI's Web and main data collection infrastructure is located in the Secaucus datacenter. The facility provides for redundant Internet connections connected to an OC-3 backbone with multiple routes to the Internet, redundant firewalls (stateful failover), managed Load balancers, redundant Managed Switches, active/active clustered web data collection and reporting servers, active/passive clustered utility servers, active/passive OLTP and OLAP database clusters, active/active IVR Application Servers, and an EMC SAN with redundant modules and hot standby disks. In addition, the facility HVAC system consist of five 600-ton chillers for distribution, 30-ton CRAC unit that are strategically located on raised floor areas, and was designed to meet N+1 redundancy requirements.

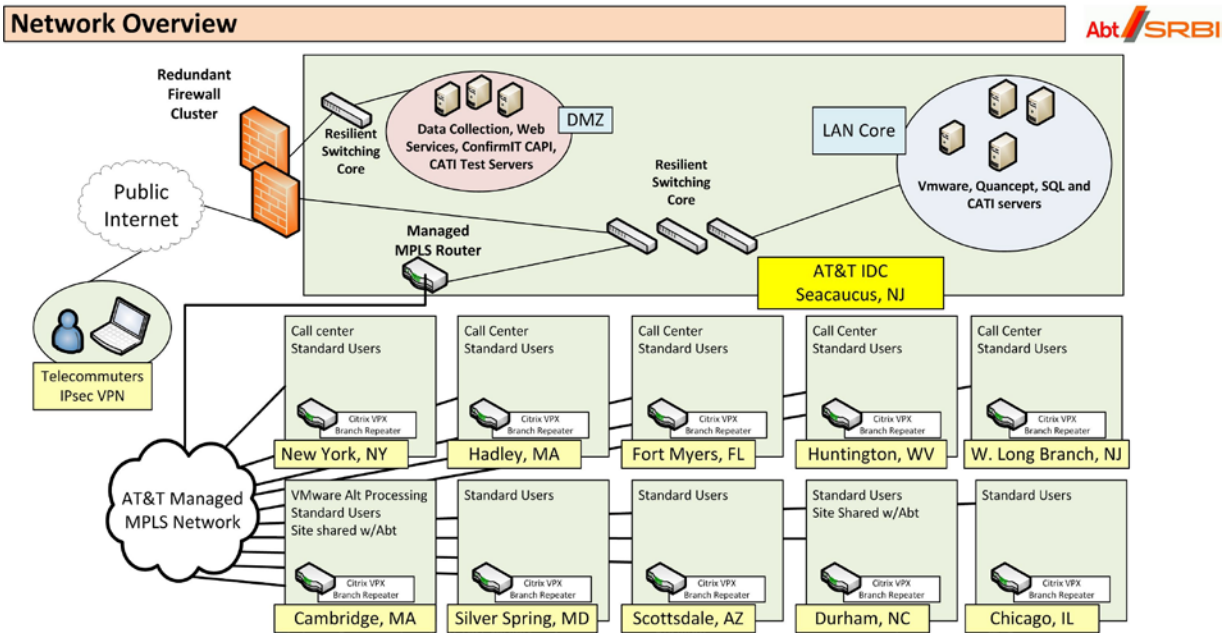
Physical security is maintained by 24-hour security guards who only allow access to pre-approved staff who must show a government-issued photo id. Guests must be announced, display a government-issued photo id, and be escorted by an authorized employee. Other guests cannot access the facility beyond the lobby which includes mantraps, electronic locks on the datacenter areas and on individual equipment cabinets. Closed circuit surveillance also covers the entire facility. Delivery personnel and couriers are only permitted access to the loading dock area to deliver equipment which is quarantined in the loading area until retrieved by an authorized employee.

In addition to the issue of protection of privacy, data security encompasses backup procedures and other file management techniques to ensure that files are not inadvertently lost or damaged. All project data files are regularly backed up to tape. File protection is additionally provided by existing procedures to prevent unauthorized changes or access to data files.

GSS Architecture

The architecture of GSS production environments is depicted in **Figure 9-2**, which shows the physical layout of the system components mapped to physical servers.

Figure 9-2: GSS Architecture



Abt SRBI Firewall

All of our Internet connections are protected by SonicWall firewalls. Firewall logs are monitored on a regular schedule and adjustments are made to ensure a high level of protection. In general, our policy is to turn off the ports for most services unless they are required to support a clearly justified business need. Access to non-standard ports is provided only after a security evaluation and with the approval of the Senior Vice President Information Technology.

Abt SRBI's datacenter firewalls are a high availability (HA) pair of SonicWall Pro E 5500. The firewalls run in FIPS 140-2 mode with gateway antivirus, anti-malware, IPS, application firewall, and centralized logging enabled. All VPN connections must meet FIPS 140-2 requirements (TDEA or AES128/256 encryption.) to connect to the SRBI network. The firewalls provide failover in the event of hardware failure. Abt SRBI allows public access only to port 80 (HTTP for web), 443 (HTTPS/SSL for secure web), 25 (SMTP e-mail), or 22 (SSH secure shell to the CATI Test System) from the public network to Abt SRBI's DMZ. Otherwise a FIPS 140-2 compliant VPN is required to access any of Abt SRBI's networks. Outside vendors are limited only to the systems which they required to access. Access from the DMZ to the LAN is not allowed except for the TCP ports required for backup services, DNS, logging, and storing information in SQL databases.

GSS Major Applications

The GSS environment is comprised of these major applications:

Confirmit Web/CAPI Data Collection Application

Abt SRBI's CAPI data collection system (**Figure 9-3**) utilizes Confirmit's data collection software to administer interviews. An interviewer in the field collects data using a laptop running Confirmit CAPI Console. That information is then sent over a secure IPSec connection or HTTPS session using server and client certificates to upload the information to Abt SRBI's secure data collection system located in the secure data center. The information is stored in a Microsoft SQL Server database for analysis using Confirmit's reporting tools.

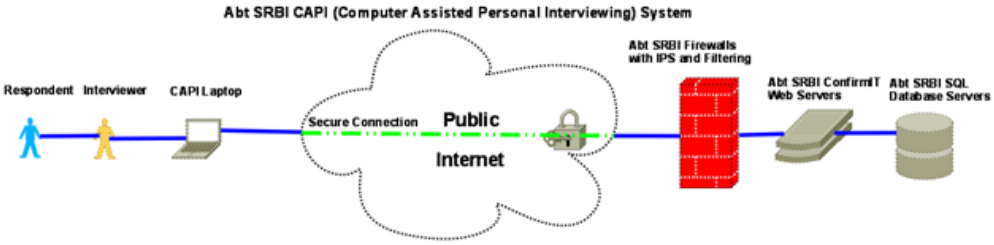


Figure 9.3: Confirmit Web/CAPI Data Collection Application Data Flow

Quancept CATI Data Collection Application

Abt SRBI's CATI data collection system (**Figure 9-4**) uses IBM's Quancept data collection software which runs on a Red Hat Linux server platform. Interviewers dial manually via analog telephones or automatically via predictive dialers depending on the needs of the project. The interviewers connect via workstations or terminals to the Red Hat servers and enter data via a terminal session.

Figure 9-4: Quancept CATI Data Collection Application Data Flow

CAWI Data Collection Application

Abt SRBI's CAWI data collection system (**Figure 9-5**) utilizes Confirmit's data collection software to administer interviews. A respondent with a computer (and a web browser with SSL capability) connects to Abt SRBI's secure survey site. The information is then sent over a secure HTTPS session to Abt SRBI's secure data collection system located in SRBI's secure data center. The information is stored in a Microsoft SQL Server database for analysis using Confirmit's reporting tools.

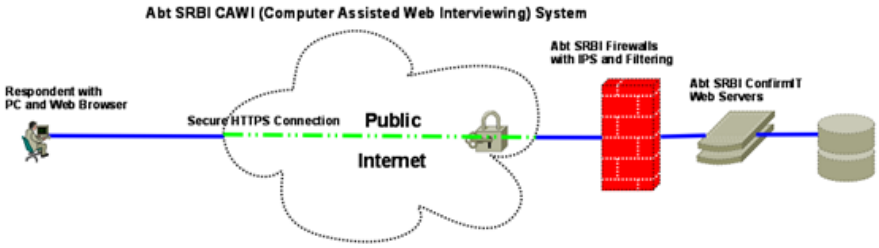


Figure 9-5: CAWI Data Collection Application Data Flow

VOXCO

Voxco is a multi-mode (CATI, CAWI, CAPI, IVR) data collection platform with robust scripting, sample management and quota management capabilities. This is accomplished through the creation of project modules that can be organized by many factors such as collection mode, sample frame, language, or even questionnaire content, while all writing to the same SQL Server database and under centralized sample management routines.

The Voxco system platform and technologies consist of several purpose-built servers each running specific components that make up the Voxco Environment (e.g. Directory server, Web Server, Agent Servers, Pronto Dialers, etc.) running on both the LAN segment and the DMZ. All LAN-side systems are joined to the production domain (SRBI.COM)

There two different hardware platforms utilized for the Voxco environment, Virtual and Physical. The physical servers are the Pronto Dialers each located on a site containing a Call Center. The Pronto Servers are HP running Dialogic Telco interfaces. The virtual servers are all located in the NJ DataCenter are running on a host platform consisting of Dell PowerEdge servers, running VMware VSphere hypervisor, and Windows 2008 R2 virtual machines. An EMC Storage Area Network (SAN) is in use to support data storage and data processing.

10. System Interconnections/Information Sharing

Interconnections among Abt SRBI Systems

The principal interconnections in the GSS are those inherent to the Company's IT environment, and described in the preceding section. These are the Company's local-area and wide-area networks; its connections to the Internet; its Virtual Private Network

In all of these cases, user access is authenticated against and controlled by a centralized and secured source: either the user profiles maintained in LDAP servers like Active Directory.

Connections between the Internet and the Company network are protected by Sonicwalls firewalls, with network controls and protections described in section 9.

Connections to Client Networks

In the event that a contract/task order requires use of a client's network or computer systems, any network connection or access to these systems will be determined based upon the access technologies the client supports.

Abt SRBI has access to and expertise in a variety of data communications technologies, and can work with clients to establish appropriate access. In the event of Abt SRBI use of a client's systems, we will develop a security plan and procedures which provide that Abt SRBI will comply with all of the client's policies and procedures regarding the use of its IT facilities.

In addition to any possible direct data communications links, electronic mail between Abt SRBI and the client will be used. All e-mail communication between the parties is subject to the confidentiality and privacy policies of both Abt SRBI and the client. Encryption can be employed when needed.

Connections to Subcontractor and Consultant Systems

In some circumstances, direct interconnections are established between Abt SRBI IT environment and trusted subcontractors, for the purpose of using subcontractor call centers for telephone survey work. Abt SRBI has had such relationships with other call centers.

Connections between Abt SRBI and these call centers are established as extranets, i.e. secure connections are established between the call centers and Abt SRBI, via either a dedicated, point-to-point leased line or the Internet. Internet-based connections between Abt SRBI and the call center are encrypted and use VPN technology, i.e. IPSEC tunnels at both ends (call center and Abt SRBI). In our Secaucus, NJ datacenter, the Survey extranet accessed by outside contractors resides on a subnet protected by an internal firewall.

No other direct network-to-network connections between Abt SRBI and its subcontractors or consultants are permitted. Abt SRBI does exchange electronic mail and files with consultants and subcontractors. The Company also provides individual remote-access services (VPN) to authorized consultant and subcontractor users. In these cases, Abt SRBI policies and procedures regarding network use, e-mail, privacy and confidentiality are applicable, as well as any additional requirements imposed by a contract, task order, or relevant law.

11. Related Laws or Regulations

Based on the information types that are processed, transmitted, and stored by Abt SRBI GSS, several laws or regulations are applicable and are listed below in chronological order of the year the law was passed. In addition, several guidelines and standards govern the implementation of the security plan.

- **Executive Order on Controlled Unclassified Information**, 4 November 2010, http://www.whitehouse.gov/the-press-office/2010/11/04/executive-order-controlled-unclassified-information
  Freedom of Information Act of 1974 (Public Law 93-502): The FOIA provides for any person to make requests for government information. All branches of the Federal government must adhere to the provisions of FOIA with certain restrictions for confidential, classified, and national security information.
- **Privacy Act of 1974 (Public Law 93-579)**: The Privacy Act of 1974 applies to the gathering and use of data by federal agencies. Virtually any database that collects information on people along with their name (and/or SSN, and/or phone number, and/or address, etc.) is subject to the provisions of this law. The Act states that such records must be protected against disclosure, auditing must be performed of changes or accesses to data, and other protections. GSS houses and transfers Privacy Act protected information.
- **Computer Fraud and Abuse Act of 1986 (Public Law 99-474)**: This Act is a law passed by the United States Congress in 1986 intended to reduce "hacking" of computer systems. It was amended in 1994, 1996 and in 2001 by the USA PATRIOT Act. The Act defines computer crime and provides for penalties regarding data stolen in computer fraud. To prosecute under this Act, GSS must provide security controls and auditing mechanisms to determine if such fraud has occurred.
- **Computer Security Act (CSA) of 1987 (Public Law 100-235)**: The Computer Security Act establishes the National Institute of Standards and Technology (NIST) as the official body to develop standards and guidelines for protection of federal information systems. It also specifies that security plans must be developed for federal systems containing “sensitive but unclassified” information and training for those who deal with those systems. Therefore, GSS uses NIST standards to develop security plan and risk assessment documentation. This Act was superseded by FISMA (2002).
- **Health Insurance Portability and Accountability Act (HIPAA) of 1996**: HIPAA was enacted by the U.S. Congress in 1996 and offers protections that improve portability and continuity of health insurance coverage for millions of American workers. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The AS provisions also address the security and privacy of health data. GSS receives and houses health data protected by HIPAA.
- **Federal Information Security Management Act (FISMA) of 2002**: The FISMA Act is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002, which extends GISRA by delegating power to the Office of Management and Budget to establish

information security policies and practices for US government agencies. Agencies are required to follow information security practices established by NIST instead of 'recommended' to 'as listed' in the CSA of 1987. Agencies and affiliated parties (such as government contractors) have to report yearly to Congress on the status of its information security compliance. As a result of this and the GISRA Act, GSS, must undergo certification and accreditation under those standards dictated by NIST.

- **Section 508 of the Rehabilitation Act**: Section 508 was enacted to eliminate barriers in information technology, to make available new opportunities for people with disabilities, and to encourage development of technologies that will help achieve these goals. Section 508 requires Federal departments and agencies that develop, procure, maintain, or use electronic and information technology to ensure that Federal employees and members of the public with disabilities have access to and use of information and data, comparable to that of the employees and members of the public without disabilities–unless it is an undue burden to do so.
- **Tax Reform Act of 1976 (Public Law 94-455) and the Taxpayer Browsing Protection Act of 1997 (HR 1226)**: The Taxpayer Browsing Protection Act provides for penalties to help ensure that taxpayers' returns and return information remain confidential. GSS contains sensitive information such as taxpayer names, Social Security Numbers, birth dates, addresses, income, filing status, exemptions. Such information is accessible only with proper authorization.
- **OMB Circular A-130**, *Management of Federal Information Resources,* Appendix III, "Security of Federal Automated Information Systems"
- **FIPS PUB 199**, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004
- **FIPS PUB 200**, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006
- **Social Security Administration**, *Information Systems Security Handbook*, version 1.5, January 11, 2007
- **NIST Special Publication 800-18 Rev. 1**, *Guide for Developing Security Plans for Information Technology Systems*, February 2006
- **NIST Special Publication 800-30**, *Risk Management Guide for Information Technology Systems*, July 2002
- **NIST Special Publication 800-37**, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, Feb 2010.*
- **NIST Special Publication 800-52**, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*, June 2005
- **NIST Special Publication 800-53 Rev. 3**, *Recommended Security Controls for Federal Information Systems and Operations*, August 2009
- **NIST Special Publication 800-53 A**, *Guide for Assessing the Security Controls in Federal Information Systems*, (third public draft)
- **NIST Special Publication 800-60**, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004

- **NIST Special Publication 800-60 Rev. 1**, DRAFT *Guide for Mapping Types of Information and Information Systems to Security Categories*, November 2008
- **NIST Special Publication 800-66**, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005
- **NIST Special Publication 800-66 Rev1**, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, May 2008

12. Minimum Security Controls

Data in the Abt SRBI GSS is treated as a **moderate** level data; this is subject to the moderate-impact baseline required by NIST Special Publication 800-53 as its minimum security control requirements.

The NIST publication specifies three general classes of security controls:

- Management controls – management of the system and management of risk;
- Operational controls – controls implemented by people; and
- Technical controls – controls executed by computer systems.

Each class contains several families of associated security controls, and each family contains several individual controls. **Table 12-1** summarizes the classes and families in the security control catalog and the associated family identifiers.

Table 12-1: Security Class and Families for a Moderate Impact System

Class	Family	Identifier	Number Of Applicable Controls
Management	Risk Assessment	RA	4
Management	Planning	PL	5
Management	System and Services Acquisition	SA	11
Management	Certification, Accreditation, and Security Assessments	CA	6
Operational	Personnel Security	PS	8
Operational	Physical and Environmental Protection	PE	18
Operational	Contingency Planning	CP	9
Operational	Configuration Management	CM	9
Operational	Maintenance	MA	6
Operational	System and Information Integrity	SI	11
Operational	Media Protection	MP	6
Operational	Incident Response	IR	8
Operational	Awareness and Training	AT	4
Technical	Identification and Authentication	IA	8
Technical	Access Control	AC	15
Technical	Audit and Accountability	AU	11
Technical	System and Communications Protection	SC	20

In the following sections of this document, we identify each of the individual controls that are applicable to a **moderate-impact** system. For each individual control identified, the control enhancements that apply are provided, per NIST SP 800-53, Revision 3.

The remainder of this chapter provides information about the applicable security controls for the Abt SRBI GSS. Details on all of the individual controls within each family and class will be developed in accordance with the overall security plan timeline.

Access Control (AC)

- Access Control Policy and Procedures (AC-1) – *Control: The organization develops, disseminates, and reviews/updates once ever twelve (12) months or when system updates necessitate: a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.*

  Control Status: In Place

  Abt SRBI has developed an Access Control Policy and Procedures document. Abt SRBI Security Team disseminates this policy as part of the annual security training provided for all users.

- Account Management (AC-2) – *Control: The organization manages information system accounts, including: a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);b. Establishing conditions for group membership; c. Identifying authorized users of the information system and specifying access privileges; d. Requiring appropriate approvals for requests to establish accounts; e. Establishing, activating, modifying, disabling, and removing accounts; f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes; h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users; i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and j. Reviewing accounts once every month. Control Enhancements: (1) The organization employs automated mechanisms to support the management of information system accounts. (2) The information system automatically terminates temporary and emergency accounts after six (6) months of inactivity. (3) The information system automatically disables inactive accounts after six (6) months of inactivity. (4) The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.*

  Control Status: In Place

  Abt SRBI creates different accounts for each user. Guest accounts are disabled by default, and accounts are disabled, not deleted, when a user either leaves the organization or is transferred. User accounts are submitted to the Abt SRBI Information Technology Network Administrators and created through the Help Desk ticket system. The Help desk maintains records of their creation or disablement.

The Abt SRBI IT department manages and maintains information system access accounts including authorizing, establishing, activating, modifying, reviewing, disabling, and removing user accounts per the AC policy and procedures. All accounts are managed in Microsoft Active directory. The HR "on-boarding" process initiates the provisioning of accounts – business units initiate the hiring and authorization process and HR communicates the authorization to IT to issue the account; the user ID is unique to the individual and policy prohibits sharing the ID. The account is provisioned with a one-time password that must be changed by the user at the first authentication. The HR "off-boarding" (termination) process initiates the de-provisioning of any accounts.

Abt SRBI IT authorizes and monitors temporary accounts using active directory. Guest accounts are not allowed.

Control Enhancement:

(1) Abt SRBI utilizes Microsoft Active Directory mechanism to manage the GSS accounts.

(2) After six (6) months of inactivity, the information system will automatically disable a user account.

(3) User accounts are disabled after six (6) months of inactivity.

(4) Account creation and modification is automatically logged and can be audited.

- Access Enforcement (AC-3) – *Control: The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.*

Control Status: In Place

The Abt SRBI GSS will utilize Discretionary Access Control (DAC) features inherent on the Windows and Linux operating system and applications to enforce access enforcement.

- Information Flow Enforcement (AC-4) – *Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.*

Control Status: In Place

Abt SRBI enforces assigned authorizations for controlling the flow of information within the Abt SRBI GSS and between interconnected systems including Data Sharing Agreements.

A Data Sharing Agreement must, at a minimum, define the following requirements:

- The identification and authentication of devices prior to establishing a connection to an Abt SRBI information network.

- The mandatory encryption and authentication requirements concerning the sending of confidential information outside the Abt SRBI environment.

- Separation of Duties (AC-5) – *Control: The organization: a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion; b. Documents separation of duties; and c. Implements separation of duties through assigned information system access authorizations.*

  Control Status: In Place

  Account types are separated based on roles, thus providing role-based access. The Abt SRBI GSS maintains a document describing the different types of accounts and their privileges and functionality.

Table 13-1 GSS Privileged User Roles

GSS Privileged User Title	Role Function
System Administrator	Responsible for supporting system administration functions of all GSS servers.
Network Administrator	Responsible for supporting system administration functions of all GSS network devices.
Database Administrator	Responsible for supporting system administration functions of all GSS databases.
Information Security Manager	Responsible for managing the GSS Security Program
Director of Information Security	Technical lead supporting responsible for managing all technical aspects of the GSS
Senior Vice President of Information Technology	Responsible for all aspects of Information Technology and Security

- Least Privilege (AC-6) – *Control: The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. Control Enhancements: (1) The organization explicitly authorizes access to system security or administrative functions. (2) The organization requires that users of information system accounts, or roles, with access to GSS system functionality, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.*

  Control Status: In Place

  The Abt SRBI GSS DAC mechanism enforces least privileges by providing (as configured by the System Owner) Privileged Users (Table 13-1 above) and general users (Table 13-2) only the least amount of access rights required to perform their necessary tasks.

Table 13-2 GSS User Roles

GSS User Title	Access Level
Research Associate	These users have limited access to the RedHat Linux systems to remotely update Confirmit and Quancept sampling data. They do not have access to Citrix or email.
Field Supervision	Field supervisors have limited access to Citrix and Abt SRBI email
Production Staff	Production staff have access to the information system only by request by the System Administrator
Project Staff	Project staff have access to the information system only by request by the System Administrator
Administrative Staff	Administrative staff have access to the information system only by request by the System Administrator

Control Enhancements:

(1) User accounts for security and administrative function is explicitly authorized by request to the system administrator and created through the Help Desk ticket system. Microsoft Discretionary Access Control (DAC) mechanism enforces these least privilege requirements.

(2) System administrators use non-privileged user accounts to perform general functions and only utilize privileged accounts when required.

- Unsuccessful Login Attempts (AC-7) – *Control: The information system: a. Enforces a limit of three (3) consecutive invalid access attempts by a user during a twenty-four (24) hour period; and b. Automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.*

  Control Status: In Place

  Abt SRBI's information system: enforces a limit of three (3) consecutive invalid access attempts by a user during a twenty-four (24) hour period. The Abt SRBI information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

- System Use Notification (AC-8) – *Control: The information system: a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: (i) displays the*

system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.

Control Status: In Place

Prior to gaining access to the information system, users are prompted with a System Use notification message. This is enforced by the login banner GPO setting. The message is as follows:

THIS COMPUTER IS OPERATED BY ABT SRBI FOR THE U.S. GOVERNMENT. BY ACCESSING AND USING THIS SYTEM YOU ARE CONSENTING TO SYSTEM MONITORING FOR LAW ENFORCEMENT AND OTHER PURPOSES. UNAUTHORIZED ACCESS TO AND/OR USE OF THIS COMPUTER SYSTEM IS A VIOLATION OF LAW AND PUNISHABLE UNDER THE PROVISIONS OF 18 U.S.C 1029, 18 U.S.C. 1030, AND OTHER APPLICABLE STATUES.

- Session Lock (AC-11) – *Control: The information system: a. Prevents further access to the system by initiating a session lock after thirty (30) minutes of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.*

  Control Status: In Place

  All windows servers and workstations are configured to automatically activate the screen saver after 15 minutes of inactivity. The user will then need to enter their password in order to disable the screen lock and gain access to the server or workstation. Connections via SSH to the Linux servers are dropped after thirty (30) minutes of inactivity. Idle time of fifteen minutes on any other interface of the system will result in a session lock.

  This is enforced through GPO:. GPO > Strategy > Administration Model > System > Power Management > Screensaver options >

- Permitted Actions without Identification or Authentication (AC-14) – *Control: The organization: a. Identifies specific user actions that can be performed on the information system without identification or authentication; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication. Control Enhancements: (1) The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.*

  Control Status: In Place

  The system does not permit any actions to take place without prior identification or authentication.

- Remote Access (AC-17) – *Control: The organization: a. Documents allowed methods of remote access to the information system; b. Establishes usage restrictions and implementation guidance for each allowed remote access method; c. Monitors for unauthorized remote access to the information system; d. Authorizes remote access to the information system prior to connection; and e. Enforces requirements for remote connections to the information system. Control Enhancements: (1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods. (2) The organization uses cryptography to protect the confidentiality and integrity of remote access sessions. (3) The information system routes all remote accesses through a limited number of managed access control points. (4) The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system. (5) The organization monitors for unauthorized remote connections to the information system on a constant basis, and takes appropriate action if an unauthorized connection is discovered. (7) The organization ensures that remote sessions for accessing system information employ authentication mechanisms and encryption mechanisms and are audited. (8) The organization disables all non-essential networking protocols except for explicitly identified components in support of specific operational requirements.*

  Control Status: In Place

  Connection to the Abt SRBI VPN is only permitted using an Abt SRBI issued computer or approved personal computer or device with the explicit prior approval from the Senior Vice President of Information Technology. Remote access to Abt SRBI environment uses multi-factor authentication. SRBI uses SonicWall E5500 to provide VPN connectivity between locations. The SonicWall E5500 is FIPS 140-2 certified. Abt SRBI deploys VASCO for 2-factor authentication. RDP connections are only allowed from computers using RDP desktop within the specified IP range.

  Control Enhancements:

  (1) The information system logs user login attempts and failures.

  (2) SonicWall's interface provides 3DES encryption during remote sessions and is FIPS 140-2 certified..

  (3) SonicWall's interface provides a single point of remote access into the information system.

  (4) Privileged commands can only be executed after authentication into a privileged account, which serves as the mechanism to restrict privileged functions from non-privileged users.

  (5) The information monitors logs for unauthorized access attempts into the system. Splunk logs continuous monitoring tracks unauthorized access to the system in the event of unauthorized access it sends an email which are reviewed twice weekly.

(7) The organization ensures that remote sessions for accessing are audited for:

- Setting/modifying audit logs and auditing behavior.
- Setting/modifying boundary protection system rules.
- Configuring/ modifying access authorizations (i.e., permissions, privileges).
- Setting/modifying authentication parameters.
  Setting/modifying system configurations and parameters employ additional authentication and encrypted channel capabilities (which is separate from remote access).

Remote access to the information system is established through the SonicWall and is FIPS 140-2 Certified. IDCS utilizes Discretionary Access Control (DAC) features inherent on Windows and Linux operating system and applications to enforce access enforcement for remote access. There are no additional security methods in use.

(8) The organization filters all other protocols and ports other than what is essential for the information system's operations.

- Wireless Access (AC-18) – *Control: The organization: a. Establishes usage restrictions and implementation guidance for wireless access; b. Monitors for unauthorized wireless access to the information system; c. Authorizes wireless access to the information system prior to connection; and d. Enforces requirements for wireless connections to the information system. Control Enhancements: (1) The information system protects wireless access to the system using authentication and encryption.*

  Control Status: Not Applicable

  - N/A. Wireless networks are not part of the system architecture and design. Abt SRBI prohibits the use of personal wireless devices attaching to the Abt SRBI network. Unauthorized devices would not be able to gain access to the Abt SRBI network without proper credentials.

- Access Control for Mobile Devices (AC-19) – *Control: The organization: a. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices; b. Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems; c. Monitors for unauthorized connections of mobile devices to organizational information systems; d. Enforces requirements for the connection of mobile devices to organizational information systems; e. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction; f. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and g. Applies formatting procedures to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures. Control Enhancements: (1) The organization restricts the use of writable, removable media in organizational information systems. (2) The organization prohibits the use of personally owned, removable media in organizational*

information systems. (3) The organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner.

Control Status: In Place

GSS laptops use Symantec End-Point on individual machines to mitigate against viruses, malware and other malicious software. Symantec End-Point also functions as the primary firewall on the laptop. All hard drives are encrypted with PGP Whole Disk encryption, which is FIPS-140-2 Certified.

Interviewer access to the Abt SRBI GSS from laptops is through a secure client/server connection. If internet connection is not available, the client will maintain the interview response in the local laptop until a connection to the internet is enabled and connection with the server is established.

- Use of External Information Systems (AC-20) – *Control: The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from the external information systems; and b. Process, store, and/or transmit organization-controlled information using the external information systems. Control Enhancements: (1) The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: (a) Can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or (b) Has approved information system connection or processing agreements with the organizational entity hosting the external information system. (2) The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.*

  Control Status: In Place

  Abt SRBI requires any external connection to sing an MOU and an ISA.

  Control Enhancement:

  (1) Abt SRBI permits an external information system to access the Abt SRBI GSS once they have been verified the implementation of the appropriate controls and have signed an MOU and an ISA.

  (2) Abt SRBI does not permit removable storage media, such as flash or thumb drives in the system.

- Publicly Accessible Content (AC-22) – *Control: The organization: a. Designates individuals authorized to post information onto an organizational information system that is publicly accessible; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information*

system; d. Reviews the content on the publicly accessible organizational information system for nonpublic information once every six (6) months; and e. Removes nonpublic information from the publicly accessible organizational information system, if discovered.

Control Status: Not Applicable

Awareness and Training (AT)

- Security Awareness and Training Policy and Procedures (AT-1) – *Control: The organization develops, disseminates, and reviews/updates at least once ever twelve (12) months or when system updates necessitate: a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.*

  Control Status: In Place

  A Security Awareness and Training policy is in place. Security Awareness training is provided annually to all Abt SRBI personnel.

- Security Awareness (AT-2) – *Control: The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and once every twelve (12) months thereafter.*

  Control Status: In Place

  The Learning Management System (LMS) documents and reports which individuals have passed the training process.

- Security Training (AT-3) – *Control: The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) annually thereafter.*

  Control Status: In Place

  The goal of the Abt SRBI Security training program is for Security Awareness training to be provided to each user specific to the role and functionality. Security training is provided prior to accessing the information system and thereafter on annual basis or when there are major changes to the system.

- Security Training Records (AT-4) – *Control: The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for twelve (12) months.*

  Control Status: In Place

The Learning Management System (LMS) is documented and reports which individuals have passed the training process and keeps the registration for the length of the users employment.

Audit and Accountability (AU)

- Audit and Accountability Policy and Procedures (AU-1) – *Control: The organization develops, disseminates, and reviews/updates at least once every twelve (12) months or when system changes necessitate: a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.*

  Control Status: In Place

  Abt SRBI does not have a specific Audit policy document. SRBI contains this information in it's Systems Operations Policy document

- Auditable Events (AU-2) – *Control: The organization: a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: error, warning and informational logs from all information system components; b. Coordinates the security audit function with other organizational entities requiring audit related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: Application and operating system critical, warning, error and information messages. Control Enhancements: (3) The organization reviews and updates the list of auditable events at least once every six (6) months. (4) The organization includes execution of privileged functions in the list of events to be audited by the information system.*

  Control Status: In Place

  The information system generates audible event logs that can be reviewed to support an after-the-fact investigation. The list of audible events have been approved and documented.

  Abt SRBI audits the following events: Account Logon Events = Not defined; Account Management = success, failure; Directory Service = No auditing; Logon Events = failure; Object Access = failure; Policy Change = success, failure; Privilege Use = failure; Process Tracking = failure; System Events = success, failure.

  Abt SRBI Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: identity of each user and device accessing or attempting to access an IT system; Time and date of the access and the logoff; Activities that might modify, bypass, or negate IT security safeguards; and Security-relevant actions associated with processing

Control Enhancements:

(3) Abt SRBI reviews audit logs on a bi-weekly basis or in the event of a security breach.

(4) Access to privileged functions is explicitly audited.

- Content of Audit Records (AU-3) – *Control: The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event. Control Enhancements: (1) The information system includes type of event, source, location and subject in the audit records for audit events identified by type, location, or subject.*

  Control status: In Place

  Abt SRBI generates audit records that support after-the-fact investigations in the event of a security incident.

  Control Enhancements:

  (1) Audit records include the type of event, source, location, and subject in each entry. These event types are generated by the Microsoft audit mechanism.

- Audit Storage Capacity (AU-4) – *Control: The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.*

  Control status: In Place

  Abt SRBI has dedicated 1.2 terabytes of storage space for audit logs. Once the space approaches 25 gigabytes of remaining space, the system will automatically generate an email alert. Audit records are backed up and stored off-site using tape drives.

- Response to Audit Processing Failures (AU-5) – *Control: The information system: a. Alerts designated organizational officials in the event of an audit processing failure; and b. Takes the following additional actions: shut down information system, overwrite oldest audit records, and stop generating audit records.*

  Control status: In Place

  In the event of an audit log failure, an automatic email is generated to the Abt SRBI Information System Security Officer. In the event of a failure such as when the system log limit is near capacity. When it is full, it will overwrite the oldest log.

- Audit Review, Analysis, and Reporting (AU-6) – *Control: The organization: a. Reviews and analyzes information system audit records once every seven (7) days for indications of*

inappropriate or unusual activity, and report findings to designated organizational officials; and b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

Control status: In Place

The system administrator manually reviews the audit logs for high priority or suspicious activity monthly.

The System administrator notifies the Information Security Manager and the Director of IT immediately in the event of inappropriate/unusual findings.

- Audit Reduction and Report Generation (AU-7) – *Control: The information system provides an audit reduction and report generation capability. Control Enhancements: (1) The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.*

  Control status: In Place

  The system currently uses Splunk to organize and sort through logs.

  Control Enhancements:

  (1) Splunk allows for events to be categorized and searched based on a logical criteria.

- Time Stamps (AU-8) – *Control: The information system uses internal system clocks to generate time stamps for audit records. Control Enhancements: (1) The information system synchronizes internal information system clocks once every thirty (30) days with authoritative time source.*

  Control status: In Place

  All audit records contain the date and time of the event. All system components use a single Windows Domain server to ensure the same time. The frequency of internal clock synchronization is set for 24 hours and is documented in Configuration Management Policy.

  Control Enhancements:

  (1) Abt SRBI's GSS synchronizes internal information system clocks at least quarterly; the United States Time source operated by NIST. Microsoft Windows automatically syncs its timestamps with the domain controllers.

- Protection of Audit Information (AU-9) – *Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.*

  Control status: In Place

Once the log is documented, only the Infrastructure Manager and Support Technician have access to them. The support Technician manually backs up the logs. General users do not have access to the audit logs.

- Audit Record Retention (AU-11) – *Control: The organization retains audit records for at least seven (7) years to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.*

  Control Status: In Place

  Abt SRBI retains audit records for at least seven (7) years to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. Audit records are retained on the information system for at least two (2) weeks. After this duration, records are archived on tape..

- Audit Generation (AU-12) – *Control: The organization retains audit records for seven (7) years to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.*

  Control Status: In Place

  The information system uses Splunk as the component for audit record generation and logging. The information system generates audit records for the auditable events that provide sufficient information to conduct after-the-fact investigations in the event of a security incident. These events are defined in control AU-2 and the content is listed in AU-3.

  Abt SRBI allows designated organizational personnel such as the Information Security Manager, the Direct of IT, the Infrastructure manager, & the SVP of IT, to select which auditable events are to be audited by specific components of the system

Certification, Accreditation, and Security Assessment (CA)

- Security Assessment and Authorization Policies and Procedures(CA-1) – *Control: The organization develops, disseminates, and reviews/updates at least on an annual basis or when changes in the information system necessitate an update: a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.*

  Control Status: In Place

  Abt SRBI does not have a specific Security Assessment policy, Abt has included these controls in the Risk Management policy and procedures unless otherwise stated.

Abt SRBI has in place a Risk Management and Assessment Policy and Procedures documents. Abt SRBI Security Team reviews, updates, & disseminates this policy annually.

- Security Assessments (CA-2) – *Control: The organization: a. Develops a security assessment plan that describes the scope of the assessment including: - Security controls and control enhancements under assessment; - Assessment procedures to be used to determine security control effectiveness; and - Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative. Control Enhancements: (1) The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.*

  Control Status: In Place

  The Abt SRBI GSS is required to meet FISMA Program requirements, including annual security assessments of all Management, Operational, and Technical security controls documented in the GSS Risk Assessment, the Security Requirements Traceability Matrix and this SSP. The Information Security Manager is required to implement NIST SP 800-53A as part of the annual security assessment. Security Assessment will be in accordance with the GSS Security Assessment Plan. Any major vulnerability discovered on the annual security assessment will require an update to the GSS Risk Assessment and the vulnerability will be documented in the GSS POA&M so that it can be tracked under the Configuration Management Program.

  Enhancement Controls:

  (1) The Abt SRBI GSS is audited by HTA, an independent assessment team against NIST 800-53 Rev 3 security controls.

- Information System Connections (CA-3) – *Control: The organization: a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements; b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.*

  Control Status: In Place

  As part of the annual security assessment, all external connections will be reviewed to ensure that agreements (MOA/MOU/ISA's) are being met by both parties. Any new connection to the system is required to get approval through the Configuration

Management Program. New connections to other organizations must be approved by the Information Security Manager.

- Plan of Action and Milestones (CA-5) – *Control: The organization: a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and b. Updates existing plan of action and milestones every ninety (90) days based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.*

  Control Status: In Place

  The vulnerabilities identified during the Certification effort, monthly vulnerability scanning, and annual assessment are documented in the POA&M. The Information Security Manager will manage the POA&M and ensure mitigation actions are completed through the Abt SRBI Configuration Management Program.

- Security Authorization (CA-6) – *Control: The organization: a. Assigns a senior-level executive or manager to the role of authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization at least once every twelve (12) months.*

  Control Status: In Place

  Abt SRBI's Senior Vice President of Information Technology has been designated as the authorizing official for the Abt SRBI GSS. The SVP of IT will review the final C&A documents..

- Continuous Monitoring (CA-7) – Control: The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: a. A configuration management process for the information system and its constituent components; b. A determination of the security impact of changes to the information system and environment of operation; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and d. Reporting the security state of the information system to appropriate organizational officials least every ninety (90) days. Control Enhancements: (1) The organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.

  Control Status: In Place

  The continuous monitoring phase consists of three tasks: (i) configuration management and control; (ii) security control monitoring; and (iii) status reporting and documentation.

  - **Configuration Management and Control:** the Abt SRBI Information Security Manager is a voting member of the Abt SRBI Change Control Board (CCB), the board responsible for approving all changes to the Abt SRBI GSS.

- **Security Control Monitoring:** Security control monitoring is supported through the following programs: Audit Reviews by the ISSO, Periodic Vulnerability Scanning, Monthly POA&M Review, Annual Security Control Assessment as documented in the Security Assessment Plan, as required by FISMA.

- **Status Reporting and Documentation**: the Abt SRBI Information Security Manager is responsible for all security documentation and reports. The SVP of IT reviews all of the supporting documents for the Abt SRBI GSS.

Configuration Management (CM)

- Configuration Management Policy And Procedures (CM-1) – *Control: The organization develops, disseminates, and reviews/updates at least once every twelve (12) months or when system updates necessitate: a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.*

  Control Status: In Place

  An approved Configuration Management Policy and Procedures document is in place.

- Baseline Configuration (CM-2) – *Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system. Control Enhancements: (1) The organization reviews and updates the baseline configuration of the information system: (a) annually as part of the Continuous Monitoring program; (b) When required due to major changes to the approved baseline configuration and when required as part of an incident response recommendation by the AO; and (c) As an integral part of information system component installations and upgrades. (3) The organization retains older versions of baseline configurations as deemed neceXXXXry to support rollback. (4) The organization: (a) Develops and maintains a list of software programs not authorized to execute on the information system]; and (b) Employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system.*

  Control Status: In Place

  The organization maintains a baseline configuration of the Abt SRBI GSS system with hardware and software configuration settings. Abt SRBI uses Virtual Machine template images as a baseline for the operating system and software configuration settings.

  Control Enhancements:
  (1) Abt SRBI does not review baseline documents, the change. System baseline documents themselves do not change; we treat them as a baseline or an "as-built' so no periodic review is necessary if a new baseline is needed than a new document incorporating all changes is built. All changes made to a system are recoded in a

"recorded changed" document outlining date, technician, change and reason. These documents would be reviewed if any system error should occur to use as a watermark for cause/effect of errors. These errors or changes are also reviewed if there are significant changes to the system and a new baseline document is needed. Abt SRBI also updates the VM template when changes become necessary due to new version of the OS, major changes to security baseline configuration or upgrades to the ESXi environment which may require new templates built.

(2) Abt SRBI maintains all versions of baseline systems and recorded changes that have occurred to that system and is able to support rollback.

(3) By default, all applications are impermissible on the system except what has been explicitly installed.

- Configuration Change Control (CM-3) – *Control: The organization: a. Determines the types of changes to the information system that are configuration controlled; b. Approves configuration-controlled changes to the system with explicit consideration for security impact analyses; c. Documents approved configuration-controlled changes to the system; d. Retains and reviews records of configuration-controlled changes to the system; e. Audits activities associated with configuration-controlled changes to the system; and f. Coordinates and provides oversight for configuration change control activities through the Configuration Control Board that convenes once every month. Control Enhancements: (2) The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.*

  Control Status: In Place

  A Configuration Control Board has been implemented by Abt SRBI. A configuration management policy and plan that meets FISMA requirements exists for Abt SRBI and its procedures are already implemented.

  Control Enhancements:

  (1) Changes to the information system are tested using a VM image and documented prior to implementation.

- Security Impact Analysis (CM-4) – *Control: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.*

  Control Status: In Place

  Prior to a change to the information system, the Abt SRBI Information Security Manager verifies that the change does not impact the security posture of the system by going through a security checklist.

- Access Restrictions for Change (CM-5) – *Control: The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.*

  Control Status: In Place

The information system defines who is allowed access to the physical environment and enforcement is carried out by AT&T.

Abt SRBI limits access to physical and logical systems currently by limiting administrative access to a small group of system administrators and facility managers.

- Configuration Settings (CM-6) – *Control: The organization: a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using a checklist specifying baseline virtual-machine specifications that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures. Control Enhancements: (3) The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.*

  Control Status: In Place

  Abt SBRI uses pre-configured VMware images as a baseline to establish configuration setting baselines. Changes to the baseline are documented on an on-going basis, including security-related concerns, changes to the system boundary, and software and hardware updates. The details behind the VMware baseline image configuration settings are documented.

  Control Enhancements:

  (2) ADAudit and Splunk monitor events. Security incidents are tracked and logged by the Help Desk tracking system. IT and Security staff correct the incidents.

- Least Functionality (CM-7) – *Control: The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: peer-to-peer technology, file-sharing utilities, or any other utilities that are not essential for the system to function. Control Enhancements: (1) The organization reviews the information system once every twelve (12) months or when business requirements change to identify and eliminate unnecessary functions, ports, protocols, and/or services.*

  Control Status: In Place

  By default, the organization disables every service, port or protocol that is not required by the servers. Each server employs a firewall to filter malicious, accidental or other unnecessary network traffic. The organization performs periodic scans to verify these settings.

Control Enhancement:

(1) Upon major changes to the system, or on an annual basis, SRBI reviews the functionality of user roles to eliminate unnecessary user privileges.

- Information System Component Inventory (CM-8) – *Control: The organization develops, documents, and maintains an inventory of information system components that: a. Accurately reflects the current information system; b. Is consistent with the authorization boundary of the information system; c. Is at the level of granularity deemed necessary for tracking and reporting; d. Includes information deemed necessary to achieve effective property accountability; and e. Is available for review and audit by designated organizational officials. Control Enhancements: (1) The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates. (5) The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.*

  Control Status: In Place

  The information system uses Wasp Mobile Asset to maintain inventory of information system components. Information system components are labeled with barcodes to ensure their unique identity.

  Control Enhancement:

  (1) Abt SRBI maintains an inventory record of the components of the information system. This list is immediately updated upon any changes to system components.

  (5) Prior to being added to the inventory list, all components are verified to be within the system boundaries.

- Configuration Management Plan (CM-9) – *Control: The organization develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.*

  Control Status: In Place

  Abt SRBI maintains a configuration management plan that specifies when changes to the information occur, who is permitted to make them, and what other conditions must take place prior to the implementation of those changes.

Contingency Planning (CP)

- Contingency Planning Policy And Procedures (CP-1) – *Control: The organization develops, disseminates, and reviews/updates at least once every twelve (12) months or when there are significant changes to the information system to necessitate an update: a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.*

  Control Status: In place

  A Contingency Policy and Procedures document is in place.

- Contingency Plan (CP-2) – *Control: The organization: a. Develops a contingency plan for the information system that: - Identifies essential missions and business functions and associated contingency requirements; - Provides recovery objectives, restoration priorities, and metrics; - Addresses contingency roles, responsibilities, assigned individuals with contact information; - Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; - Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the contingency plan to key contingency personnel; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system once every twelve (12) months; e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and f. Communicates contingency plan changes to key contingency personnel. Control Enhancements: (1) The organization coordinates contingency plan development with organizational elements responsible for related plans.*

  Control Status: Planned

  Abt SRBI has developed a Contingency Policy. However a plan is currently not in place.

  Control Enhancements:
  (1) Contingency planning is coordinated with all personnel who would be involved in the reconstitution of the system through a table top exercise.

- Contingency Training (CP-3) – *Control: The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training at least once every twelve (12) months or when there are significant changes to the contingency plan.*

  Control Status: In Place

Abt SRBI provides contingency training in the event of a security incident and annually to those employees involved in the CP process.

- Contingency Plan Testing and Exercises (CP-4) – *Control: The organization: a. Tests and/or exercises the contingency plan for the information system once every six (6) months using a table-top exercise to determine the plan's effectiveness and the organization's readiness to execute the plan; and b. Reviews the contingency plan test/exercise results and initiates corrective actions. Control Enhancements: (1) The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.*

  Control Status: Planned

  The organization performs table-top exercises with key disaster recovery individuals to simulate the actions taken after a security incident or disruption of services.

  Control Enhancement:

  (1) Abt SRBI performs contingency plan testing through a table top exercise with all parties who are involved in the reconstitution of the system.

- Alternate Storage Site (CP-6) – *Control: The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information. Control Enhancements: (1) The organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards. (3) The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.*

  Control Status: In Place

  The dedicated alternate storage site is located in West Long Branch, New Jersey.

  Control Enhancements:

  (1) The alternate storage side is in West Long Branch, New Jersey.

  (2) The alternate storage site is geographically separated far enough that an area-wide disaster would not affect it.

- Alternate Processing Site (CP-7) – *Control: The organization: a. Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within forty-eight (48) hours when the primary processing capabilities are unavailable; and b. Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption. Control Enhancements: (1) The organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards. (2) The organization identifies potential accessibility problems to the alternate processing site in*

the event of an area-wide disruption or disaster and outlines explicit mitigation actions. (3) The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements. (5) The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.

Control Status: In Place

Abt SRBI has an established alternate processing site at it's Cambridge MA location .

Control Enhancements:

(1) Abt SRBI's Cambridge MA is separated from the primary site by approximately 215 miles, which enables it not to be susceptible to the same hazards as the primary site.

(2) The alternate processing site is an Abt SRBI office, in the event of accessibility problems the site will be moved to another Abt SRBI office, these are detailed in the CP policy and procedures documents

(3) The alternate processing site is an Abt SRBI office, all agreements are in place

(5) The Abt SRBI alternate processing site is an existing Abt SRBI facility and provides equivalent physical and logical security measures equivalent to that of the primary site.

- Telecommunications Services (CP-8) – *Control: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within seven (7) days when the primary telecommunications capabilities are unavailable. Control Enhancements: (1) The organization: (a) Develops primary and alternate telecommunications service agreements that contain priority of- service provisions in accordance with the organization's availability requirements; and (b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier. (2) The organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.*

Control Status: In Place

Abt SRBI does not have a centrally located telecommunications service. Service for all locations is done by local provider. Redundancy is provided by ability to use whatever provider is available.

Control Enhancements:

(1) Abt SRBI uses an alternate ISP in the event that a single connection fails; this service is provided by the data center.

(2) Abt SRBI's alternate ISP was acquired with the awareness that it is intended to reduce the possibility of a single point of failure.

- Information System Backup (CP-9) – *Control: The organization: a. Conducts backups of user-level information contained in the information system on a nightly basis; b. Conducts backups of system-level information contained in the information system on a nightly basis; c. Conducts backups of information system documentation including security-related documentation on a nightly basis; and d. Protects the confidentiality and integrity of backup information at the storage location. Control Enhancements: (1) The organization tests backup information on a nightly basis to verify media reliability and information integrity.*

  Control Status: In Place

  The system performs daily incremental and weekly full backups. The backup are transported to alternate site weekly.

  Control Enhancements:

  (1) Backups are tested on a monthly basis to verify information integrity.

- Information System Recovery and Reconstitution (CP-10) – *Control: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Control Enhancements: (2) The information system implements transaction recovery for systems that are transaction-based. (3) The organization provides compensating security controls for circumstances that can inhibit recovery and reconstitution to a known state.*

  Control Status: In Place

  In the event of a loss of data, Abt SRBI can rebuild the database with the last snapshot. The databases are configured to allow transaction-based roll-back.

  Abt SRBI hosts the GSS in a VMware environment and Abt SRBI regularly maintains system snapshots. In the event of a system failure, Abt SRBI seamlessly transfers the VM image to another physical machine to continue operations and uploads current backup data.

  Control Enhancements:

  (2) The system databases use transaction-based logs that can reconstitute a database to a known state. Baselines nightly are performed on a weekly basis.

  (3) The organization performs baseline backups to prevent against corrupted transaction logs.

Identification and Authentication (IA)

- Identification and Authentication Policy and Procedures (IA-1) – *Control: The organization develops, disseminates, and reviews/updates at least once every twelve (12) months or when significant system updates necessitate: a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.*

  Control Status: Planned

  An Identification and Authentication Policy and Procedures document is in place.

- Identification and Authentication (Organizational Users) (IA-2) – *Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). Control Enhancements: (1) The information system uses multifactor authentication for network access to privileged accounts. (2) The information system uses multifactor authentication for network access to non-privileged accounts. (3) The information system uses multifactor authentication for local access to privileged accounts. (8) The information system uses secure forms of encryption for network access to privileged accounts.*

  Control Status: In Place

  Each user has a unique user account. Each user must be on an Abt SRBI approved device and using an Abt SRBI IP address. There are no shared users..

  Control Enhancement:

  (1) Multifactor (password and token) access is only required for privileged (administrative) and non-privileged remote access to systems. Internal access to privileged accounts does not require multifactor authentication.

  (2) Multifactor (password and token) access is only required for privileged (administrative) and non-privileged remote access to systems. Internal access to privileged accounts does not require multifactor authentication.

  (3) The system does not implement two-factor authentication for local access.

  (8) Abt SRBI uses SSL/TLS as it's replay-resistant mechanism. The SSL/TLS channel itself protects against replay attacks using the MAC, computed using the MAC secret and the sequence number. To prevent message replay or modification attacks, the MAC is computed from the MAC secret, the sequence number, the message length, the message contents, and two fixed character strings.

- Device Identification and Authentication (IA-3) – *Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). Control Enhancements: (1) The information system uses multifactor authentication for*

network access to privileged accounts. (2) The information system uses multifactor authentication for network access to non-privileged accounts. (3) The information system uses multifactor authentication for local access to privileged accounts. (8) The information system uses replay-resistance encryption algorithms for network access to privileged accounts.

Control Status: In Place

IP address and if required MAC addresses filtering at the SonicWall switch can be utilized to support this control.

- Identifier Management (IA-4) – *Control: The organization manages information system identifiers for users and devices by: a. Receiving authorization from a designated organizational official to assign a user or device identifier; b. Selecting an identifier that uniquely identifies an individual or device; c. Assigning the user identifier to the intended party or the device identifier to the intended device; d. Preventing reuse of user or device identifiers for five (5) years; and e. Disabling the user identifier after ninety (90) days of inactivity.*

  Control Status: In Place

  Network accounts are disabled after 90-days of inactivity. Sessions that are left inactive for 30-minutes are locked and must be re-authenticated into. User accounts are not deleted; they are disabled indefinitely to facilitate an after-the-fact investigation.

- Authenticator Management (IA-5) – *Control: The organization manages information system authenticators for users and devices by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators upon information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate); g. Changing/refreshing authenticators every five (5) years; h. Protecting authenticator content from unauthorized disclosure and modification; and i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators. Control Enhancements: (1) The information system, for password-based authentication: (a) Enforces minimum password complexity of one non-alphanumeric character, one number, one upper-case character, one lower-case and at least seven characters in length; (b) Enforces at least a seven characters in length when new passwords are created; (c) Encrypts passwords in storage and in transmission; (d) Enforces password minimum and maximum lifetime restrictions of sixty (60) days; and (e) Prohibits password reuse for five (5) generations. (2) The information system, for PKI-based authentication: (a) Validates certificates by constructing a certification path with status information to an accepted trust anchor; (b) Enforces authorized access to the corresponding private key; and (c) Maps the authenticated identity to the user account. (3) The organization requires that the registration process to receive username and password authenticators be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).*

Control Status: In Place

Minimum complexity requirements are forced by the system, users are forced to change the initial password on first successful log-in, initial log-in is provided to the new user by IT either in person or by phone if the user is remote. Default system passwords are changed upon implementation.

Control Enhancements:
(1) Abt SRBI has documented password sensitivity in the AC Policy document
(2) Certificates must be validated by created a path to a trust-anchor. Otherwise, they are not accepted for use by the information system.
(3) Usernames and passwords are given to users by the network administrator or IT Support staff only after the Abt SRBI supervisor and human resources department have authorized access to the system.

- Authenticator Feedback (IA-6) – *Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.*

  Control Status: In Place

  In the event of a failed login, the information system responds with "Access Denied", thus not disclosing if a username exists. All passwords are masked to prevent an onlooker from observing the password.

  Masking of passwords is required for all operating systems and applications requiring users to identify and authenticate prior to access. Abt SRBI GSS utilizes Windows and Linux Operating System mechanism for authenticator feedback. When a user enters their password on a Windows or Linux host, the operating system masks the password so it cannot be seen. Currently all other applications utilized by GSS is supporting the enforcement of this requirement. New applications will be required to go through the CCB and Security Engineers will ensure that future application requests enforce this requirement.

- Cryptographic Module Authentication (IA-7) – *Control: The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.*

  Control Status: In Place

  Abt SRBI requires user ID and password pair authentication when using encryption to backup the database or distribute files. The database is archived with AES and files are encrypted with PGP. All encryption algorithms are FIPS 140-2 certified for Windows XP. SRBI also uses a cryptographic module to authenticate users in the SonicWall E5500 firewall, which is FIPS140-2 certified. .

- Identification and Authentication (Non-Organizational Users) (IA-8) – *Control: The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).*

  Control Status: In Place

  Abt SRBI does not allow any non-organizational users access to the system.

Incident Response (IR)

- Incident Response Policy and Procedures (IR-1) – *Control: The organization develops, disseminates, and reviews/updates once every twelve (12) months or when system updates necessitate: a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.*

  Control Status: In Place

  Abt SRBI has developed formal Incident Identification and Response policy and procedures documents. Abt SRBI reviews and updates these documents annually

- Incident Response Training (IR-2) – *Control: The organization: a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and b. Provides refresher training once every twelve (12) months or when system updates necessitate.*

  Control Status: In Place

  Training is identified in the Security Training and Testing Policy and Procedures documents and is implemented and tracked via the LMS system or by the Information Security department. Training is annual and encompasses all current material in the Incident Identification and Response documents.

- Incident Response Testing and Exercises (IR-3) – *Control: The organization tests and/or exercises the incident response capability for the information system once every twelve (12) months using scenarios developed by the security officer to determine the incident response effectiveness and documents the results.*

  Control Status: In Place

  Abt SRBI has implemented an Incident Identification and Response Policy and Procedures, and testing is completed every 365 days. The test are defined in the Incident Identification and Response policy and procedures and the Security training and testing documents. Results and lessons learned documents are created and reviewed to help determine the validity of each test. .

- Incident Handling (IR-4) – *Control: The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment,*

eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly. Control Enhancements: (1) The organization employs automated mechanisms to support the incident handling process.

Control Status: In Place

In the event of a security incident, end-users will send an email to the Help Desk to create a ticket. A security ticket will go to the Information Security Manager. If there was a security breach, the SVP of IT is notified. In this situation, within 24-hours, the client will be notified.

Control Enhancement:

(1) In the event of a security breach, audit records help capture the event. Incidents are tracked through the Help Desk tracking system.

- Incident Monitoring (IR-5) – *Control: The organization tracks and documents information system security incidents.*

  Control Status: In Place

  Abt SRBI tracks and monitors security incidents through their Help Desk system. The Help Desk system does not hold sensitive or cleared information.

- Incident Reporting (IR-6) – *Control: The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within twenty-four (24) hours; and b. Reports security incident information to designated authorities. Control Enhancements: (1) The organization employs automated mechanisms to assist in the reporting of security incidents.*

  Control Status: In Place

  Users are trained to contact the Help Desk when reporting a security incident. Abt SRBI's Help Desk ticket system provides reporting on security incidents that are delivered to the SVP of IT and the Information Security Manager at least once a week or on an ad-hoc basis. All incident reporting is delivered to the SVP of IT, the Information Security Manager, and to the client within 24-hours.

  Control Enhancement:

  (1) Security incidents are tracked and reported through the Help Desk tracking system.

- Incident Response Assistance (IR-7) – *Control: The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security*

incidents. Control Enhancements: (1) The organization employs automated mechanisms to increase the availability of incident response related information and support.

Control Status: In Place

In the event of a security breach, the affected area is taken off-line and it is given the top priority. The Information Security Manager is the main resource involving security incidents

Control Enhancements:

(1) Incidents are tracked through the Help Desk ticket system.

- Incident Response Plan (IR-8) – *Control: The organization: a. Develops an incident response plan that: - Provides the organization with a roadmap for implementing its incident response capability; - Describes the structure and organization of the incident response capability; - Provides a high-level approach for how the incident response capability fits into the overall organization; - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; - Defines reportable incidents; - Provides metrics for measuring the incident response capability within the organization. - Defines the resources and management support needed to effectively maintain and mature an incident response capability; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the incident response plan to Information System Security Officer and System Administrator; c. Reviews the incident response plan at least once every twelve (12) months or when major system updates necessitate; d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and e. Communicates incident response plan changes to organizational incident response personnel.*

Control Status: In Place

Security incidents are handled immediately by isolating the event, removing the threat if possible, performing an investigation to determine what occurred, and to minimize the impact to the confidentiality, availability and integrity. Afterwards, the system is updated to prevent a future security incident.

Maintenance (MA)

- System Maintenance Policy and Procedures (MA-1) – *Control: The organization develops, disseminates, and reviews/updates at least once a year or when changes to the information system necessitate: a. A formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.*

Control Status: In Place

System Operations Policy and Procedures documents are in place.

- Controlled Maintenance (MA-2) – *Control: The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions. Control Enhancements: (1) The organization maintains maintenance records for the information system that include: (a) Date and time of maintenance; (b) Name of the individual performing the maintenance; (c) Name of escort, if necessary; (d) A description of the maintenance performed; and (e) A list of equipment removed or replaced (including identification numbers, if applicable).*

  Control Status: In Place

  System maintenance is performed in a controlled environment. By default, system maintenance is performed in-house by Abt SRBI personnel. The objective, time and nature of the maintenance is documented. In the event an external resource is required, in addition to the previous requirements, visitors are required to sign in and present photographic identification, must be escorted at all time, and their activities on the system are constantly monitored.

  Control Enhancements:

  (1) The Network Administrators keep maintenance records for the Abt SRBI GSS which include: date and time of maintenance, name of the individual preforming maintenance, description of work performed, and a list of equipment replaced or removed.

- Maintenance Tools (MA-3) – *Control: The organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools. Control Enhancements: (1) The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications. (2) The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.*

  Control Status: In Place

  Abt SRBI provides its own software and hardware tools used during system maintenance and update. In the event external individuals are required for system maintenance, those resources are not permitted to use software or hardware that is capable of recording system data. In the event that external resources require internet access, they are provided with a guest area, separate from the Abt SRBI DMZ LAN without any form of access to the LAN.

Control Enhancement:

(1) Abt SRBI maintains a list of tools that are permitted into the server room.

(2) All software tools are tested to ensure that there is no malicious code in them.

- Non-Local Maintenance (MA-4) – *Control: The organization: a. Authorizes, monitors, and controls non-local maintenance and diagnostic activities; b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions; d. Maintains records for non-local maintenance and diagnostic activities; and e. Terminates all sessions and network connections when non-local maintenance is completed. Control Enhancements: (1) The organization audits non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions. (2) The organization documents, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections.*

  Control Status: In Place

  Remote maintenance is performed through VPN. Maintenance auditing is generated through the VPN's auditing system. Non-local users will create a temporary account that will be deleted immediately after their work is created.

  Control Enhancement:

  (1) Non-local system maintenance is logged and monitored.

  (2) Non-local tools and connections are documented.

- Maintenance Personnel (MA-5) – *Control: The organization: a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed neceXXXXry to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.*

  Control Status: In Place

  Abt SRBI maintains a list of which individuals are granted access to their information systems. Only those individuals are granted access to the information system for maintenance purposes. Other resources do not have access to the Abt SRBI GSS.

- Timely Maintenance (MA-6) – *Control: The organization obtains maintenance support and/or spare parts for information system components within forty-eight (48) hours of failure.*

  Control Status: In Place

Abt SRBI hosts the Abt SRBI GSS in a VMware environment and Abt SRBI regularly maintains system snapshots. In the event of a system failure, Abt SRBI seamlessly transfers the VM image to another physical machine to continue operations. Abt SRBI performs software updates on an on-going basis. If a software update requires the system to be shutdown, this is scheduled with GSS personnel and performed during non-peak hours.

Media Protection (MP)

- Media Protection Policy and Procedures (MP-1) – *Control: The organization develops, disseminates, and reviews/updates once every twelve (12) months or when system updates necessitate: a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.*

  Control Status: In Place

  Abt SRBI has produced Media Protection Policy And Procedures documents. Abt SRBI reviews and updates these documents annually. The Abt SRBI Security Team disseminates this policy as part of the annual security training provided for all users.

- Media Access (MP-2) – *Control: The organization restricts access to information system digital and non-digital media to all but non-project specific personnel. Control Enhancements: (1) The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.*

  Control Status: In Place

  Abt SRBI restricts access of PII to non-project specific cleared individual. This is done by not allowing them access to the information system, which contains this information.

  Control Enhancement:

  (1) All system data is protected by user permissions, preventing non-authorized users from creating media. Additionally, the system does not have a monitor or printer attached to generate media output.

- Media Marking (MP-3) – *Control: The organization: a. Marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts removable media from marking as long as the exempted items remain within the server room and environment.*

  Control Status: In Place

  Abt SRBI has a classification marking policy in place for the collection, distribution and destruction of PII, PHI, Public, Proprietary, and Restricted data

- Media Storage (MP-4) – *Control: The organization: a. Physically controls and securely stores information system electronic data within the production, processing and backup locations using sufficiently strong encryption; b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.*

  Control Status: In Place

  Backup media is stored in an off-site location, all media is destroyed prior to release.

- Media Transport (MP-5) – *Control: The organization: a. Protects and controls all digital and non-digital media, including presentations, documents and paperwork during transport outside of controlled areas using strong encryption or non-transparent coverings and concealments; b. Maintains accountability for information system media during transport outside of controlled areas; and c. Restricts the activities associated with transport of such media to authorized personnel. Control Enhancements: (2) The organization documents activities associated with the transport of information system media. (4) The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.*

  Control Status: In Place

  Media is transported by authorized Abt SRBI personnel between the data center and the alternate storage facility. All tapes are cataloged and an inventory is maintained.

  Control Enhancement:

  (2) All transport of media must be logged, and specified with what it contains, who is the transporter, and the dates of departure and receipt.

  (4) Electronic data is encrypted with PGP Cryptographic engine 4.0 during transport. PGP is FIPS 140-2 certified

- Media Sanitization (MP-6) – *Control: The organization sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse.*

  Control Status: In Place

  Abt SRBI currently using DBAN, will wipe over a hard drive 7 times. The person doing the sanitizing must fill out the form, including the system name, model, serial number, what the destruction method is. There is a double-watch policy that says who must be visible while this is done.

  Tapes are degaussed and reused. If they are on CD or paper, they are shredded

Physical and Environmental Protection (PE)

- Physical and Environmental Protection Policy and Procedures (PE-1) – *Control: The organization develops, disseminates, and reviews/updates at least once every twelve (12) months or when physical conditions change: a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.*

  Control Status: In Place

  Abt SRBI has a physical and environmental protection policy. Abt SRBI Security Team disseminates this policy as part of the security training provided for all users every 365 days.

- Physical Access Authorizations (PE-2) – *Control: The organization: a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); b. Issues authorization credentials; c. Reviews and approves the access list and authorization credentials at least once every twelve (12) months or when the physical conditions of the information system change, removing from the access list personnel no longer requiring access.*

  Control Status: In Place

  Access to the information system is restricted to approved personnel and this list in maintained in accordance to Abt SRBI's access control policy. Users are only granted access after the sensitivity of the position has been reviewed. Once they are hired by the company, access to the system is restricted to the minimum requirements. In Abt SRBI offices only reception areas are publicly accessible. All other areas require ID badge or visitor sign in and escort. In the AT&T Datacenter, AT&T maintains a preapproved list of current personnel with authorized access to the Abt SRBI Data center co-located in AT&T's facility in Secaucus, NJ. Only the Abt SRBI SVP of IT and Director of IT can approve visitors to the facility. They must be escorted at all times.

- Physical Access Control (PE-3) – *Control: The organization: a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible); b. Verifies individual access authorizations before granting access to the facility; c. Controls entry to the facility containing the information system using physical access devices and/or guards; d. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk; e. Secures keys, combinations, and other physical access devices; f. Inventories physical access devices at least once every twelve (12) months or when system inventories change; and g. Changes combinations and keys at least once every six (6) months and when keys are lost, combinations are compromised, or individuals are transferred or terminated.*

  Control Status: In Place

Physical access to the information is restricted to only those users who have been granted prior access by the Abt SRBI SVP of IT or the Director of IT. The server room is guarded twenty-four hours a day by AT&T dedicated security staff. Before access is granted, users must present both (government issued) photographic identification and pass through a biometric authentication.

The facility is monitored 24 hours, 7 days a week by on-site professional security guards and monitored over continuous closed circuit video surveillance from a command center via both stationary and 360° cameras located both outside and inside the facility.

- Access Control for Transmission Medium (PE-4) – *Control: The organization controls physical access to information system distribution and transmission lines within organizational facilities.*

  Control Status: In Place

  The servers are guarded by either biometric or bolt locks. Telephony and internet cables are guarded by AT&T dedicated security staff and are located behind physical barriers.

- Access Control for Output Devices (PE-5) – *Control: The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.*

  Control Status: In Place

  Physical access to the information output devices is restricted to only those users who have been granted prior access by the Abt SRBI SVP of IT or the Director of IT and kept in the secure datacenter facility..

- Monitoring Physical Access (PE-6) – *Control: The organization: a. Monitors physical access to the information system to detect and respond to physical security incidents; b. Reviews physical access logs once a week; and c. Coordinates results of reviews and investigations with the organization's incident response capability. Control Enhancements: (1) The organization monitors real-time physical intrusion alarms and surveillance equipment.*

  Control Status: In Place

  Physical security is maintained by 24-hour AT&T security guards who only allow access to pre-approved staff who must show a government-issued photo id. Guests must be announced, display a government-issued photo id, and be escorted by an authorized employee. Other guests cannot access the facility beyond the lobby which includes mantraps, electronic locks on the datacenter areas and on individual equipment cabinets.

  The facility is monitored 24 hours, 7 days a week by on-site professional security guards and monitored over continuous closed circuit video surveillance from a command center via both stationary and 360° cameras located both outside and inside the facility.Control Enhancements:

(1) The facility is monitored 24 hours, 7 days a week by on-site professional security guards and monitored over continuous closed circuit video surveillance from a command center via both stationary and 360° cameras located both outside and inside the facility.

- Visitor Control (PE-7) – *Control: The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible. Control Enhancements: (1) The organization escorts visitors and monitors visitor activity, when required.*

  Control Status: In Place

  Physical security is maintained by 24-hour AT&T security guards who only allow access to pre-approved staff who must show a government-issued photo id. Access to the information is restricted to only those users who have been granted prior access by the Abt SRBI SVP of IT or the Director of IT. Guests must be announced, are required to sign a visitor log, present a government-issued photo id, pass through a biometric verification, and must be escorted at all times by authorized personnel who have escort privileges to the facility.. Other guests cannot access the facility.

  Control Enhancement:
  (1) All visitors must be escorted and monitored during their visit.

- Access Records (PE-8) – *Control: The organization: a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and b. Reviews visitor access records at least once every seven (7) days.*

  Control Status: In Place

  Abt SRBI maintains visitation access records for seven (7) years and Security Officer or designee reviews visitor logs weekly in the event of a security incident.

- Power Equipment and Power Cabling (PE-9) – *Control: The organization protects power equipment and power cabling for the information system from damage and destruction.*

  Control Status: In Place

  The information system power cabling are stored behind concrete walls and only available at electrical access points.

- Emergency Shutoff (PE-10) – *Control: The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in the server environment to facilitate safe and easy*

access for personnel; and c. Protects emergency power shutoff capability from unauthorized activation..

Control Status: In Place

Emergency shut-off switches are located at the AT&T hosting facility.

- Emergency Power (PE-11) – *Control: The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.*

  Control Status: In Place

  In the AT&T datacenter UPS provide continuous power for all equipment in the datacenter and a generator provides alternative electric power to the entire building should local utility power fail. Individual UPS' are provided for each server rack.

- Emergency Lighting (PE-12) – *Control: The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.*

  Control Status: In Place

  In the event of a power outage or disruption, AT&T provides automated emergency lighting in the entire data center, including all emergency exits and evacuation routes.

- Fire Protection (PE-13) – *Control: The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source. Control Enhancements: (1) The organization employs fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire. (2) The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders. (3) The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.*

  Control Status: In Place

  AT&T employs a smoke detection and a fire suppression system in case of a fire that are automatically engaged in case of smoke and/or fire. In the event of a fire, the sprinkler system produces an audible sound and Emergency responders and appropriate personnel are automatically notified.

  Control Enhancements:

  (1) AT&T employs a smoke detection and a fire suppression system in case of a fire that are automatically engaged in case of smoke and/or fire. In the event of a fire, the

sprinkler system produces an audible sound and Emergency responders and appropriate personnel are automatically notified..

(2) The Data Center uses non-charged, localized sprinkler systems to suppress fire.

(3) The AT&T data center is staffed 24/, however the smoke and fire suppression system is automated and does not require staffing.

- Temperature and Humidity Controls (PE-14) – *Control: The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at every five (5) minutes; and b. Monitors temperature and humidity levels every five (5) minutes.*

  Control Status: In Place

  AT&T follows the Abt SRBI policy and maintains an adequate temperature of 65-75°F with a humidity level of 40 to 50 percent within the data center where information systems resides. The AT&T datacenter maintains Computer Room Air Conditioning (CRAC) units. The CRAC units are strategically located near the computer cage and racks and deliver conditioned air. They regulate and monitor the temp and humidity. The room temperature is kept at approximately 75degrees.

- Water Damage Protection (PE-15) – *Control: The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.*

  Control Status: In Place

  The Data Center does not house water pipes near the information system. The Data Center overhead sprinkler system includes a pre-action dry pipe system and is only triggered in the event of a fire or emergency. There is a master shutoff valve in the data center for any water that is in the building. The AT&T building facility personnel control the master shut off valves.

- Delivery and Removal (PE-16) – *Control: The organization authorizes, monitors, and controls flash drives, portable cellular phones, disks, CDs, and any other device that can store digital media entering and exiting the facility and maintains records of those items.*

  Control Status: In Place

  AT&T tracks any part that is delivered to the datacenter facility and any part that is carried in. Only parts that are preregistered for delivery or brought by an approved source are permitted. Abt SRBI Information system components are tracked using Wasp Mobile asset. Individual components are assigned a bar-code for unique identification.

- Alternate Work Site (PE-17) – *Control: The organization: a. Employs management, operational, and technical information system security controls at alternate work sites; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for*

employees to communicate with information security personnel in case of security incidents or problems.

Control Status: Not In Place

Abt SRBI has designated the Abt SRBI Cambridge, MA office as an alternate works site. Abt SRBI employs management, operational, and technical information system security controls at the Cambridge site. These are reviewed annually. .

- Location of Information System Components (PE-18) – *Control: The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.*

  Control Status: In Place

  Abt SRBI's AT&T data center locates information components away from locations that are prone to flood and water damage, flammable locations, such as loose papers and any environmental hazards. Abt SRBI's information system components are located in a fully enclosed locked cage in the AT&T datacenter to protect from unauthorized access.

  Physical security is maintained by 24-hour AT&T security guards who only allow access to pre-approved staff who must show a government-issued photo id. Guests must be announced, display a government-issued photo id, and be escorted by an authorized employee. Other guests cannot access the facility beyond the lobby which includes mantraps, electronic locks on the datacenter areas and on individual equipment cabinets. Closed circuit surveillance also covers the entire facility. Delivery personnel and couriers are only permitted access to the loading dock area to deliver equipment which is quarantined in the loading area until retrieved by an authorized employee.

Planning (PL)

- Security Planning Policy and Procedures (PL-1) – *Control: The organization develops, disseminates, and reviews/updates at least once every twelve (12) months or when major changes in the system necessitate such changes: a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.*

  Control Status: In Place

  A Security Planning Policy is in place.

- System Security Plan (PL-2) – *Control: The organization: a. Develops a security plan for the information system that: - Is consistent with the organization's enterprise architecture; - Explicitly defines the authorization boundary for the system; - Describes the operational context of the information system in terms of missions and business processes; - Provides the security category and impact level of the information system including supporting rationale; - Describes the operational environment for the information system; - Describes relationships with or*

connections to other information systems; - Provides an overview of the security requirements for the system; - Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and - Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Reviews the security plan for the information system on an annual basis or when significant changes to the system take place; and c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

Control Status: In Place

The Abt SRBI SSP meets the requirements identified under PL-2.

- Rules of Behavior (PL-4) – *Control: The organization: a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.*

  Control Status: In Place

  Before any user, either general or privileged, is granted access to Abt SRBI GSS, they will be required to go through security awareness training and at the completion of the training will sign the Abt SRBI Rules of Behavior form. Annually thereafter, both general and privileged users will re-sign the Abt SRBI Rules of Behavior form after annual training has been performed.

- Privacy Impact Assessment (PL-5) – *Control: The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.*

  Control Status: In Place

  A Privacy Threshold Assessment (PTA) is completed for most major projects on the GSS

- Security-Related Activity Planning (PL-6) – *The organization develops, monitors, and reports on the results of information security measures of performance.*

  Control Status: In Place

  Before changes are made to the information system, Abt SRBI performs a security impact and operations assessment to make sure that the changes do not adversely affect the confidentiality, availability or integrity of the information system. All changes are made through the Change Control Board and documented. Security monitoring results will be incorporated into the Plan of Action and Milestones

Personnel Security (PS)

- Personnel Security Policy and Procedures (PS-1) – C*ontrol: The organization develops, disseminates, and reviews/updates at least once every twelve (12) months or when updates and changes to the system necessitate a review/update: a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.*

  Control Status: In Place

  Abt SRBI has developed a Personnel Security Policy and Procedures document. SRBI Security Team disseminates this policy as part of the annual security training provided for all users.

- Position Categorization (PS-2) – *Control: The organization: a. Assigns a risk designation to all positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and revises position risk designations at least once every five (5) years.*

  Control Status: In Place

  Positions are identified, as well as the risk designations and requirements that must be met to fill the related positions.

- Personnel Screening (PS-3) – *Control: The organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals every five (5) years and prior to employment.*

  Control Status: In Place

  Abt SRBI's HR department performs personnel background on new resources to determine if the level of risk associated with granting access to the new employee is acceptable. Abt SRBI does not re-screen employees unless specifically stated in a contract.

  As part of the Abt SRBI Information Security Manager's duties he has the responsibility to notify the Abt Human Resources Director if there are reasons to believe that a cleared person has violated the standards of conduct or has exhibited behavior that would lead another reasonable person to conclude that the reliability or suitability of that individual is in question.

- Personnel Termination (PS-4) – *Control: The organization, upon termination of individual employment: a. Terminates information system access; b. Conducts exit interviews; c. Retrieves all security-related organizational information system-related property; and d. Retains access to*

organizational information and information systems formerly controlled by terminated individual.

Control Status: In Place

Upon termination of an employee, information system access to the employee is removed; the employee must comply with an exit interview, and return all information system assets. Abt SRBI HR conducts exit interviews with every terminated employee.

- Personnel Transfer (PS-5) – *Control: The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates transfer or reassignment actions within one day of formal transfer.*

  Control Status: In Place

  If a transfer occurs, HR notifies all relevant departments including Information Technology which adjusts the user permissions appropriately.

- Access Agreements (PS-6) – *Control: The organization: a. Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access; and b. Reviews/updates the access agreements at least once every twelve (12) months or when significant changes in access agreements necessitate a formal review.*

  Control Status: In Place

  Before new users are granted permissions onto the Abt SRBI GSS , they are provided an on boarding training by HR and sign authorization agreements that they will abide by all information system policies and usage guidance. This is handled by the Human Relations department at Abt SRBI. The Abt SRBI HR department is responsible for this on an annual basis. All new users are also required to attend the Security Awareness training prior to accessing any systems.

- Third-Party Personnel Security (PS-7) – *Control: The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Documents personnel security requirements; and c. Monitors provider compliance.*

  Control Status: In Place

  Third-Party personnel are required to meet all security requirements, and must have a signed MOU and an ISA in place.

- Personnel Sanctions (PS-8) – Control: The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

  Control Status: In Place

Users that do not comply with acceptable use policy will have their access to the information system terminated.

Risk Assessment (RA)

- Risk Assessment Policy and Procedures (RA-1) – Control: The organization develops, disseminates, and reviews/updates every twelve (12) months: a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

  Control Status: In Place

  Risk Management and Assessment Policy and Procedures documents are in place.

- Security Categorization (RA-2) – *Control: The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.*

  Control Status: In Place

  Abt SRBI documents the security categorization results (including supporting rationale) in the System Security Plan (SSP) and other project documents (including a Baseline System Information (BSI) documents) for the information systems and ensures the security categorization decision is reviewed and approved per applicable Federal agency requirements..

- Risk Assessment (RA-3) – *Control: The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in risk assessment report; c. Reviews risk assessment results once every three (3) years; and d. Updates the risk assessment once every three (3) years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.*

  Control Status: In Place

  An initial Risk Assessment was completed on September 15, 2010 by HTA and updated as of October 16, 2013, an independent security consulting firm

- Vulnerability Scanning (RA-5) – *Control: The organization: a. Scans for vulnerabilities in the information system and hosted applications at least once every three (3) years, when there are major changes to the system and at random intervals and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for: - Enumerating platforms, software flaws, and improper configurations; - Formatting and making transparent, checklists and test procedures; and - Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities immediately or within a six (6) month period in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). Control Enhancements: (1) The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.*

  Control Status: In Place

  Vulnerability scans are run weekly and ad-hoc by the Abt SRBI Information Security Manager. Legitimate vulnerabilities are remediated within 48 hours, if they that cannot be remediated within 48 hours they are added to the Plan of Action and Milestones (POA&M).

  Control Enhancements:

  (1) Nessus uses Common Vulnerability Enumeration (CVE) nomenclature for many different processes. All vulnerabilities identified by Tenable's research group for the Nessus vulnerability scanner or the Passive Vulnerability Scanner have relevant CVE entries (if available). The NVD (National Vulnerabilities Database) is used by Tenable to provide scores within the Nessus plugins. .

System and Service Acquisition (SA)

- System and Services Acquisition Policy and Procedures (SA-1) – C*ontrol: The organization develops, disseminates, and reviews/updates at least once every twelve (12) months or when major system changes necessitate: a. A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.*

  Control Status: In Place

  Abt SRBI has in place a Security Development Policy document. Abt SRBI reviews and updates this policy annually. Abt SRBI Security Team disseminates this policy as part of the annual security training. .

- Allocation of Resources (SA-2) – *Control: The organization: a. Includes a determination of information security requirements for the information system in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.*

  Control Status: In Place

  Resources are determined, documented and allocated based on system/mission requirements.

- Life Cycle Support (SA-3) – *Control: The organization: a. Manages the information system using a system development life cycle methodology that includes information security considerations; b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and c. Identifies individuals having information system security roles and responsibilities.*

  Control Status: In Place

  Abt SRBI has developed a System Development Life Cycle.

- Acquisitions (SA-4) – *Control: The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards: a. Security functional requirements/specifications; b. Security-related documentation requirements; and c. Developmental and evaluation-related assurance requirements. Control Enhancements: (1) The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls. (4) The organization ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.*

  Control Status: In Place

  SRBI will ensure all system specific acquisition for GSS is in accordance with procurement guidance and will meet federal laws, Executive orders, directives, policies, regulations, and standards.

  Control Enhancements:

  (1) The purpose and function of each component is documented and approved by Abt SRBI prior to purchase.

  (4) Each new component approved by Abt SRBI management prior to purchase and is explicitly assigned and tracked to the Abt SRBI GSS.

- Information System Documentation (SA-5) – *Control: The organization: a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes: - Secure configuration, installation, and operation of the information system; - Effective use and maintenance of security features/functions; and - Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and b. Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes: - User-accessible security features/functions and how to effectively use those security features/functions; - Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and - User responsibilities in maintaining the security of the information and information system; and c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent. Control Enhancements: (1) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing. (3) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.*

  Control Status: In Place

  System documentation will be provided to Abt SRBI personnel who require access to them to complete their tasks and responsibilities. Update and dissemination of system specific documentation will be the responsibility of the Abt SRBI Senior Netwrok administrators and Director of IT, while the Information Security Manager will be responsible for the update and dissemination of security related documentation (such as this SSP).

  Control Enhancement:

  (1) Abt SRBI maintains vendor documents describing the information system components and their implementation within the system.

  (3) Abt SRBI maintains a high-level diagram describing the role of each component in the information system.

- Software Usage Restrictions (SA-6) – *Control: The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.*

  Control Status: In Place

Abt SRBI has a list of approved software and restricts users from installing additional software.

- User-Installed Software (SA-7) – *Control: The organization enforces explicit rules governing the installation of software by users.*

  Control Status: In Place

  Abt SRBI has a list of approved software. General users are not able to install additional software without approval from Abt SRBI and without administrator privileges.

- Security Engineering Principles (SA-8) – *Control: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.*

  Control Status: In Place

  Abt SRBI technical security personnel are involved in the secure design and provide support on any changes to the Abt SRBI GSS.

- External Information System Services (SA-9) – *Control: The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Monitors security control compliance by external service providers.*

  Control Status: In Place

  As required by the Abt SRBI Security Development Policy, Abt SRBI Must:
  - Require that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
  - Define and document oversight and user roles and responsibilities with regard to external information system services.
  - Monitor security control compliance of external service providers through annual assessments, as defined in the Risk Management Policy and Risk Management Procedures.

- Developer Configuration Management (SA-10) – *Control: The organization requires that information system developers/integrators: a. Perform configuration management during information system design, development, implementation, and operation; b. Manage and control changes to the information system; c. Implement only organization-approved changes; d. Document approved changes to the information system; and e. Track security flaws and flaw resolution.*

Control Status: In Place

In the event of a change to the information system, project managers will develop and execute an implementation plan. If these plans require system downtime, Abt SRBI will negotiate an appropriate time with the all affected parties. All changes, flaws and errors are tracked through Abt SRBI's Helpdesk tracking system.

- Developer Security Testing (SA-11) – *Control: The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers): a. Create and implement a security test and evaluation plan; b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and c. Document the results of the security testing/evaluation and flaw remediation processes.*

  Control Status: In Place

  Abt SRBI only utilizes COTS products, so there is no flaw remediation process. If the COTS products had an issue, Abt SRBI would contact the manufacturer and either request a work-around or use the most appropriate manor to mediate the issue.

System and Communications Protection (SC)

- System And Communications Protection Policy And Procedures (SC-1) – *Control: The organization develops, disseminates, and reviews/updates at least once every twelve (12) months or when system updates necessitate: a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.*

  Control Status: In Place

  Abt SRBI has developed a System and Communication Protection Policy and Procedures document. SRBI Security Team will disseminate this policy as part of the annual security training provided for all users.

- Application Partitioning (SC-2) – *Control: The information system separates user functionality (including user interface services) from information system management functionality.*

  Control status: In Place

  System administrators use a general account for day-to-day operations; general users do not have administrative rights to their workstations. By design, Microsoft partitions its software through the use of Active Directory permissions, and Group Policy Objects (GPOs), which actively separate user and information system management functionality.

- Information in Shared Resources (SC-4) – *Control: The information system prevents unauthorized and unintended information transfer via shared system resources.*

Control status: In Place

Users do not have administrator privileges on the laptops and are not able to install peer-to-peer software. The firewall rules do not allow outbound users to connect to machines within the DMZ. By design, Microsoft prevents unauthorized and unintended information transfer via shared system resources through Active Directory permissions, and Group Policy Objects (GPOs).

- Denial of Service Protection (SC-5) – *Control: The information system protects against or limits the effects of the following types of denial of service attacks: [ICMP floods, Teardrop attacks, application floods, malformed packets leading to system crashes (Nukes), Distributed Denial of Service attacks, or other forms of DoS attacks.*

  Control status: In Place

  Abt SRBI's information system protects against or limits the effects of the following types of denial of service attacks: as defined in NIST 800-61 Rev. 1 or Common Vulnerabilities and Exposures (CVE), including Bandwidth/ network, protocol/ services, and software/systems. Denial of Service (DoS) protections is provided at the perimeter by Abt SRBI firewalls. The information system is protected by several layers. AT&T provides hosting for the Abt SRBI servers, whose Cisco routers mitigate against DoS attacks by dropping packets that follow a DoS attack signature. Secondly, the default SonicWall E5500 rules filter against known DoS attack signatures. Third, Abt SRBI uses load-balancing between for its public-facing servers. Finally, Symantec's Endpoint firewall drops packets that meet known DoS attack signatures.

- Boundary Protection (SC-7) – *Control: The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and b. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. Control Enhancements: (1) The organization physically allocates publicly accessible information system components to separate sub-networks with separate physical network interfaces. (2) The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices. (3) The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic. (4) The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; (e) Reviews exceptions to the traffic flow policy at least every six (6) months or when significant changes in the system necessitate a formal review; and (f) Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need. (5) The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception). (7) The information system prevents remote devices that have established a*

non-remote connection with the system from communicating outside of that communications path with resources in external networks.

Control status: In Place

The boundary is protected by SonicWall E5500. This is documented in the Firewall Details document. The firewall filters all inbound connections, except port 80 and 443. Outbound connections are not filtered.

Control Enhancements:

(1) The information system is enclosed within a separate rack and is protected by a lock.

(2) Abt SRBI does not allow public access into it's internal network except as appropriately mediated by VPN and 2 factor authentication. .

(3) All remote users must authenticate onto the system through a single SonicWall appliance.

(4) Remote users interface with the SonicWall client. Abt SRBI IT utilizes FIPS 140-2 compliant mechanism(s) to protect the integrity and confidentiality of transmitted information

(5) By default, firewalls deny everything but connections on port 80 and 443. Outbound connections are not filtered. Systems requiring direct access from the internet are hosted in the DMZ.

(7) Remote users are not able to establish a non-remote connection with the GSS by communicating outside of the appropriate means of traffic flow within the system.

- Transmission Integrity (SC-8) – *Control: The information system protects the integrity of transmitted information. Control Enhancements: (1) The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.*

  Control status: In Place

  Transmissions are protected by SonicWall's VPN client, which utilizes both TDEA and AES-128 and AES-256 encryption.

  Communication between the Abt SRBI site offices via the AT&T MPLS is encrypted to prevent other customers from accessing the GSS communication.

  Enhancement Control:

  (1) Local connections are secured through AT&T's MPLS system. SSL provides data integrity in transit by calculating a message digest.

- Transmission Confidentiality (SC-9) – *Control: The information system protects the confidentiality of transmitted information. Control Enhancements: (1) The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.*

  Control status: In Place

  Transmissions are protected by SonicWall's VPN client, which utilizes both TDEA and AES-128 and AES-256 encryption a mix of PGP and PKI.

  Communication between the Abt SRBI site offices via the AT&T MPLS is encrypted to prevent other customers from accessing the GSS communication. Remote maintenance is performed using SSH, which utilizes SSL version 2.0.

  Enhancement Controls:

  (1) Transmissions are protected by SonicWall's VPN client, which utilizes both TDEA and AES-128 and AES-256 encryption, a mix of PGP and PKI.

- Network Disconnect (SC-10) – *Control: The information system terminates the network connection associated with a communications session at the end of the session or after no more than thirty (30) minutes of inactivity.*

  Control Status: In Place

  Unix SSH systems terminate session after 15 minutes; Windows systems require re-authentication to reinitiate a session. Web sessions do not maintain keep-alive and therefore drop immediately after web-data is delivered.

- Cryptographic Key Establishment and Management (SC-12) – *Control: The organization establishes and manages cryptographic keys for required cryptography employed within the information system.*

  Control Status: In Place

  GSS uses encryption in multiple areas. To encrypt files during transportation and on the hard-drive of the laptops, the information system employs PGP and PGP Whole Disk encryption. VPN connectivity to the system is encrypted using a pre-shared certificate. Web-based connection to the system is encrypted using IPSec or SSL. Keys are managed automatically by PGP and SSl the keys and initial vectors are all generated by the application at the time of connection. Key generation is then managed by the device itself.

- Use of Cryptography (SC-13) – *Control: The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.*

Control Status: In Place

Abt SRBI uses MOVEit DMZ by Ipswitch for SFTP transmissions which have been certified as meeting or exceeding FIPS 140-2 requirements.

- Public Access Protections (SC-14) – *Control: The information system protects the integrity and availability of publicly available information and applications.*

  Control Status: In Place

  Public does not have access to this system.

- Collaborative Computing Devices (SC-15) – *Control: The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: administrative maintenance over VPN, Windows Remote Desktop or similar means of collaborative tools; and b. Provides an explicit indication of use to users physically present at the devices.*

  Control Status: Not Applicable

  GSS does not have any, nor support, collaborative computing

- Public Key Infrastructure Certificates (SC-17) – *Control: The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.*

  Control Status: In Place

  While Abt SRBI GSS does not use PKI, PKI is installed on the machine. The root-certificate on the machine is up to date and using a secure hashing algorithm.

- Mobile Code (SC-18) – *Control: The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system.*

  Control Status: Not Applicable

  CAPI laptop users have Client Side .NET installed. This is an authorized installation.

- Voice Over Internet Protocol (SC-19) – *Control: The organization: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of VoIP within the information system.*

  Control Status: In Place

Abt SRBI only issues VoIP devices to authorized Abt SRBI personnel for telecommunications only. SRBI IT allows only approved devices on the VoIP segments of the network and incorporates continuous VoIP monitoring into the Abt SRBI audit capabilities. Abt SRBI VoIP is only used for internal communications, except for VPN using 2 factor authentication.

GSS uses VoIP through AT&T's dedicated (Multiprotocol Label Switching) MPLS infrastructure for communication between site offices for telecommunications only. Abt SRBI does not monitor VoIP communications. See figure 13-5

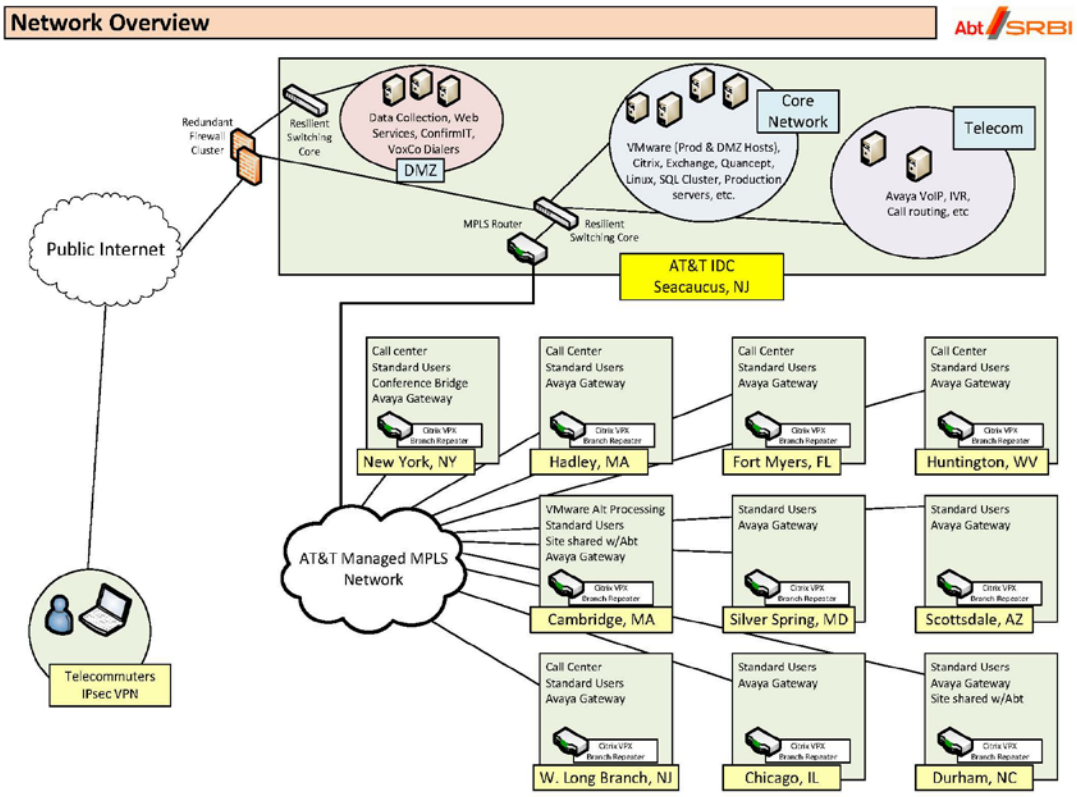


Figure 13-5 Abt SRBI GSS Network and Data Flow Diagram

- Secure Name/Address Resolution Service (Authoritative Source) (SC-20) – *Control: The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries. Control Enhancements: (1) The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.*

  Control status: In Place

Abt SRBI uses E-Directory and Active Directory Integrated DNS..

- Architecture and Provisioning for Name/Address Resolution Service (SC-22) – *Control: The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.*

  Control status: In Place

  Both internal and external DNS servers are redundant. As part of the AT&T services, DNS have multiple failovers to ensure DNS services are maintained. Abt SRBI has primary and backup DNS servers. Abt SRBI only provides DNS services internally, and does not provide any DNS services externally. See SC-20. Internal host are pointed to an internal DNS.

- Session Authenticity (SC-23) – *Control: The information system provides mechanisms to protect the authenticity of communications sessions.*

  Control status: In Place

  Communications sessions are protected by VPN, IPsec and SSL. IPsec communication is certified with certificates provided by VeriSign and GoDaddy. Web servers utilize only server side certs for encryption. Server authentication is not performed.

- Protection of Information at Rest (SC-28) – *Control: The information system protects the confidentiality and integrity of information at rest.*

  Control status: In Place

  For information at rest, Abt SRBI ensures proper access controls and permissions to files and folders. Abt SRBI installs PGP whole disk encryption on all laptops.

- Information System Partitioning (SC-32) – *Control: The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.*

  Control status: In Place

  The Abt SRBI is on a flat architecture. Other than the DMZ, all servers are on the same subnet. Workstations connecting to IDCS from remote offices are on separate subnets. .

System and Information Integrity (SI)

- System and Information Integrity Policy and Procedures (SI-1) – *Control: The organization develops, disseminates, and reviews/updates at least once every twelve (12) months or when system updates necessitate: a. A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the*

implementation of the system and information integrity policy and associated system and information integrity controls.

Control Status: In Place

Information Integrity Policy and Procedures documents are in place.

- Flaw Remediation (SI-2) – *Control: The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and c. Incorporates flaw remediation into the organizational configuration management process. Control Enhancements: (2) The organization employs automated mechanisms at least once every six (6) months to determine the state of information system components with regard to flaw remediation.*

  Control Status: In Place

  In the event of an identified flaw in the system, Abt SRBI will contact either the vendor, if the flaw is specific to an application, or will identify the configuration-related issue and construct a solution. Abt SRBI will test the solution on a VMWare test image to check for possible errors.

  Control Enhancement:

  (1) GSS is scanned with Nessus on a weekly basis to determine whether flaws have been eliminated from the system.

- Malicious Code Protection (SI-3) – *Control: The organization: a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: - Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or - Inserted through the exploitation of information system vulnerabilities; b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: - Perform periodic scans of the information system once every seven (7) days and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and - block malicious code, quarantine malicious code and send alert to administrator in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Control Enhancements: (1) The organization centrally manages malicious code protection mechanisms. (2) The information system automatically updates malicious code protection mechanisms (including signature definitions). (3) The information system prevents non-privileged users from circumventing malicious code protection capabilities.*

  Control Status: In Place

Abt SRBI employs several mechanisms to prevent malicious code from entering the system. At the network parameter, Abt SRBI uses SonicWall E5500 to filter out malicious traffic. Individual Windows machines use Symantec Endpoint to filter for viruses and other malicious code. Email is filtered for Viruses and other malicious code by Microsoft Hosting Services. Linux machines do not use any anti-virus software.

Control Enhancements:

(1) Abt SRBI uses Symantec Endpoint

(2) Symantec Endpoint's malicious code protection signatures are automatically updated on a weekly basis.

(3) Symantec Endpoint cannot be uninstalled by non-administrative users.

- Information System Monitoring (SI-4) – *Control: The organization: a. Monitors events on the information system in accordance with the ability to reconstruct the mechanics of an attack and detects information system attacks; b. Identifies unauthorized use of the information system; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations. Control Enhancements: (2) The organization employs automated tools to support near real-time analysis of events. (4) The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions. (5) The information system provides near real-time alerts when the following indications of compromise or potential compromise occur: virus scanner, IDS, IPS and firewalls. (6) The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.*

  Control Status: In Place

  Abt SRBI monitors unauthorized use of GSS by using a SonicWall E5500, a stateful inspection firewall with built-in high-speed gateway anti-virus, anti-spyware, intrusion prevention and powerful deep packet inspection capabilities. The traditional firewall controls are supplemented with a Sonicwall application level firewall, which delivers the aforementioned deep packet inspection..

  The SonicWall is configured between the Internet and the GSS to monitor inbound and outbound traffic. SonicWall provides near real time e-mail alerts when a potential malicious traffic is identified. Symantec Endpoint is also used to protect the system and is centrally managed.

  This control is implemented through Solar Wind IP Monitor and Deep Packet Inspection.

(2) SonicWall Audit Log viewer and Splunk are used to view security incidents in real time.

(4) Inbound and outbound traffic are monitored using SonicWall.

(5) The SonicWALL device also incorporates a logging feature, which can be utilized from the same configuration web browser-based session. Several reports can be generated from the same interface, including bandwidth usage by protocol, bandwidth usage by IP address, and sites generating the most traffic.In the event fo a detected intrusion attempt, SonicWall will send an automatic email to the system administrator and continue to log

(6) All traffic is routed through a single channel, so non-privileged users are not able to circumvent security monitoring.

- Security Alerts, Advisories, and Directives (SI-5) – *Control: The organization: a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to the Information System Security Officer and System Administrator; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.*

  Control Status: In Place

  The Abt SRBI Information Security manager maintains a list of sites to monitor, based on technology implemented in GSS that will provide security alerts identifying latest patches, hot fixes, and services packs for software utilized in GSS operating systems and applications. When these alerts are received, the GSS Security Manager will develop a GSS internal alert, advisory, or directive to be sent to the System Administration staff.

  Abt SRBI administrators subscribe to US CERT and CVE for daily updates on security-related issues.

  When received, Abt SRBI Security Manager will ensure that the GSS technical staff reacts to security related alerts and advisories within 30 days otherwise it will be added to the POA&M for tracking.

- Software and Information Integrity (SI-7) – *Control: The information system detects unauthorized changes to software and information. Control Enhancements: (1) The organization reassesses the integrity of software and information by performing monthly integrity scans of the information system.*

  Control Status: In Place

  Abt SRBI uses ADAudit plus and Nessus to scan for changes to the information system. Symantec Endpoint and Windows File Protection are active on some servers. The information system undergoes weekly scans to ensure that there are no new

vulnerabilities on the system. This is performed with Nessus Symantec Endpoint and Windows File Protection are active on the Confirm-It servers.

Control Enhancement:

- (1) The information system undergoes weekly scans to ensure that there are no new vulnerabilities on the system. This is performed with

- Nessus.Spam Protection (SI-8) – *Control: The organization: a. Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited meXXXXges transported by electronic mail, electronic mail attachments, web accesses, or other common means; and b. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.*

  Control Status: In Place

  For Abt SRBI internal email system Abt SRBI SPAM filtering is handled by Microsoft's Forefront managed service. Microsoft's Forefront managed service updates the spam protection mechanism when new releases are available.

- Information Input Restrictions (SI-9) – *Control: The organization restricts the capability to input information to the information system to authorized personnel.*

  Control Status: In Place

  Handled by Confirm-It at the application level. At the field level, the databases are set up to be user friendly. If the field requires numerical values, it will not accept alpha-characters.

- Information Input Validation (SI-10) – *Control: The information system checks the validity of information inputs.*

  Control Status: In Place

  Handled by the Confirm-It application, constraints are set on specific tables by the administrators.

- Error Handling (SI-11) – *Control: The information system: a. Identifies potentially security-relevant error conditions; b. Generates error messages that provide information necessary for corrective actions without revealing application-design information in error logs and administrative messages that could be exploited by adversaries; and c. Reveals error messages only to authorized personnel.*

  Control Status: In Place

  No de-bugging strings or system specific error messages are revealed to the user.

- Information Output Handling and Retention (SI-12) – *Control: The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.*

  Control Status: In Place

  All output from the Abt SRBI GSS will be handled For Official Use Only until validated that it contains no PII data or sensitive data. If the output contains PII data, hardcopies will be locked up when not in use and digital copies encrypted utilizing FIPS 140-2 approved NIST certified encryption mechanism.

  Positive control of the PII or sensitive data must be maintained at all times until either transferred to an authorized source or properly destroyed in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements..

Attachment A. Referenced Acronyms

Acronym	Definition
Admin	Information Technology Administrator
CAPI	Computer Assisted Personal Interview
C&A	Certification & Accreditation
CISO	Chief Information Security Officer
COTS	Common Off The Shelf
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GSS	General Support System
GOTS	Government Off The Shelf
HIPAA	Health Insurance Portability and Accountability Act
LDAP	Lightweight Directory Access Protocol
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
PHI	Protected Health Information
SDLC	System Development Life Cycle
SSO	Single Sign-On
SysAdmin	System Administrator
URL	Uniform Resource Locator
WBS	Work Breakdown Structure

Attachment B. Rules of Behavior Form

Every user must:

- Be familiar with current information on security, privacy and confidentiality practices.
- Obtain written authorization before using sensitive or critical applications.
- Use only systems and data for which they have authorization.
- Lock or logoff their workstation/terminal prior to leaving it unattended.
- Act in an ethical, informed and trustworthy manner.
- Protect sensitive electronic records.
- Be alert to threats and vulnerabilities to their systems.

Every manager must:

- Monitor use of mainframes, PCs, LANs, and networked facilities to ensure compliance with national and local policies.
- Ensure that employee screening for sensitive positions within their components has occurred prior to any individual being authorized access to sensitive or critical applications.
- Implement, maintain and enforce systems security standards and procedures;
- Immediately contact their security officer whenever a systems security violation is discovered or suspected.
- Employees who fail to adequately safeguard personally identifiable information by failing to secure it from theft, loss or inadvertent disclosure may be subject to disciplinary action.

Applicability

The responsibility to protect personally identifiable information applies at all times regardless of whether Abt SRBI employees, grantees, or contractors.

Examples of Failing to Safeguard Personally Identifiable Information

The following list provides examples of situations where personally identifiable information is not properly safeguarded:

- Leaving an unprotected computer containing sensitive or restricted information in an non-secure space (e.g., leaving the computer unattended in a public place, in an unlocked room, or in an unlocked car);
- Leaving a claims folder open and unattended on one's desk in a non-secure area, including any place where the public visits;
- Leaving an unattended briefcase containing sensitive or restricted information in a non-secure area, including any place in the office;

- Storing electronic files containing sensitive or restricted information on a computer or access device (flash drive, CD, etc.) that other people have access to (not password-protected);
- Working from home with a file containing personally identifiable information but not locking the file in a secure file cabinet when not being used.

This list does not encompass all failures to safeguard personally identifiable information but alerts employees to situations that must be avoided. Misfeasance occurs when an employee is authorized to access or possess sensitive or restricted information that contains sensitive or personally identifiable information and, due to the employee's failure to exercise due care, the information is lost, stolen or inadvertently released.

Whenever you have doubts about a specific situation involving your responsibilities for safeguarding personally identifiable information, you should consult your supervisor or the Information Security Manager.

Print Name	Signature	Date