Information Technology System Security Plan

Abt SRBI Inc.
275 Seventh Ave, Suite 2700
New York, NY 10001

March 5, 2009

Prepared by

Dwight A. Feanny
Director of Information Technology

Information Technology System Security Plan
Table of Contents

1.0 **EXECUTIVE SUMMARY**

This Information Technology System Security Plan 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, *Guide for Developing Security Plans for Information Technology Systems,* 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.

All data-related work conducted under government contracts involves use of Abt SRBI IT environment, which is the Company's general support system (GSS). This plan describes the practices and controls by which Abt SRBI maintains the security, confidentiality, integrity and availability of all client and internal data stored and processed within the GSS. It is the master security plan for Abt SRBI, and all contract work is subject to these controls. In cases where a government agency, contract or task order has security requirements that exceed the controls specified in this plan, an additional security plan, for that "Major Application", would be developed that addresses the agency or contract-specific requirements.

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.

2.0 SYSTEM IDENTIFICATION

2.1 System Name/Title

Abt SRBI Inc. Information Technology (IT) Environment.

2.2 Responsible Organization

Information Technology Department
Abt SRBI Inc.
275 Seventh Ave, Suite 2700
New York, NY 10001

2.3 Information Contacts

2.3.1 System Owner

Mr. Albert Ronca
Chief Operating Officer
Abt SRBI Inc.
275 Seventh Ave, Suite 2700
New York, NY 10001

2.3.2 Business Steward

Ms. Mindy Rhindress
Senior Vice President
Abt SRBI Inc.
275 Seventh Ave, Suite 2700
New York, NY 10001

2.3.3 Technical Stewards

For WAN and LAN connections services and end-user computing:

Mr. Christopher M. Williams
Manager of Information Technology
Abt SRBI Inc.
7431 College Parkway
Fort Myers, Florida 33907
(239) 278-4044

For Security:
Mr. Dwight A. Feanny
Vice President, Director of Information Technology
Abt SRBI Inc.
275 Seventh Ave, Suite 2700
New York, NY 10001
(212)-779-7700

2.4 System Category

The Abt SRBI IT Environment consists of the general support system (GSS).

The GSS includes the Abt SRBI main Secaucus data center and computer rooms in its other offices; the Company's microcomputer hardware, software and local-area networks (LANs); a wide-area network (WAN) that connects the Company's offices; connections between Abt SRBI offices and the Internet; and a virtual private network (VPN) providing secure, encrypted connectivity across the Internet. The capabilities provided by the GSS, which are supported from our data center in Secaucus, multiple call centers (New York, NY; Fort Myers, FL; West Long Branch, NJ; Huntington WV; Hadley, MA), and branch offices are as follows:

- File and print services
- Office automation services (e.g. electronic mail; word processing; spreadsheets; presentation graphics)
- Internet services (e.g. Web browsing, SFTP, telnet)
- Statistical analysis
- Network communications
- Computer-aided telephone interviewing (CATI)
- Interactive Voice Response system (IVR)
- Computer aided personal Interviewing (CAPI) and web surveys

.

2.5 Assignment of Security Responsibility

The Security Stewards are:

Mr. Christopher Williams (WAN & perimeter security)
Manager of Information Technology
Abt SRBI Inc.
7431 College Parkway
Fort Myers, Florida 33907
(239-278-4044)

Mr. Edward Ashcraft (Novell/LAN Security)
Senior Network Administrator
Abt SRBI Inc.
7431 College Parkway
Fort Myers, Florida 33907
(239) 278-4044

Mr. Frank Sfalanga (Linux Systems Security)
Manager of Information Technology
Abt SRBI Inc.
7431 College Parkway
Fort Myers, Florida 33907
(239-278-4044)

2.6 System Operation Status

The system is operational.

2.7 General Description/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; 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.

2.7.1 Application Overview

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. These include:

Electronic mail and messaging: Novell GroupWise v. 7.0

Office automation: Microsoft Office 2003 and 2007 Suite

Web browsing: Microsoft Internet Explorer 6 & 7; Adobe Acrobat Reader; Mozilla Firefox

Statistical analysis: SPSS is the Company-standard statistical package. Other statistical packages are used when required by specific projects. These include SUDAAN, SAS, MapInfo and BrandMap
.
Utility software: DBMS Copy, WinZip, TextPad, CuteFTP, Symantec Corporate Anti-Virus, PGP and others

Survey applications: SPSS Quancept for CATI; Confirmit Web for web surveys; PulseTrain Ltd. Fusion system, for CATI and CAPI surveys; Apex for IVR surveys

Custom applications may be developed depending upon the requirements of a contract/task order. In this case and where appropriate, a separate security plan is developed for the application.

2.7.2 Operating Environment/Platforms

Abt SRBI operates a data center in Secaucus, NJ, and satellite computer rooms in its other offices (New York, NY; Silver Springs, MD; Fort Myers, FL; West Long Branch, NJ; Erlanger, KY; Scottsdale, AZ; Huntington, WV; Chicago, IL; Hadley, MA; Durham, NC; Cambridge, MA). The data center and satellite computer rooms are comprised of a multi-vendor environment, with the following platforms in use:

- Electronic mail: Novell GroupWise 7.0, running on Dell servers with Novell Netware v. 6.5.
- File services: Novell Netware v. 6.5 running on Dell file servers.
- Directory services: Novell eDirectory 8.7.3 (LDAP service) and Microsoft Active Directory.
- Authentication services: NMAS authentication running under Novell Netware v. 6.5.
- Firewall services: Sonicwall Pro Appliances.
- Statistical packages – host based: SPSS v. 15.0 running on a Dell server.
- Statistical packages – PC-based: SPSS v. 15.0.
- Statistical packages – PC-based: Sudaan v. 8.
- Survey data collection systems: PulseTrain Fusion system, running on Windows 2003 servers with MS SQL 2005 back-end databases; Quancept 7.8/7.9, running on Redhat ES Linux; Apex IVR, running on Windows 2000 and 2003 servers with MS SQL 2000 back-end databases; Confirmit Web, running on Windows 2003 servers with MS SQL 2005 back-end databases.

The Company also operates approximately 150 PC's that are used for e-mail, office automation and statistical data analysis. The PC operating systems primarily in use are Windows 2000 & XP Pro. The PCs themselves include a wide range of Dell Dimension and Optiplex desktop systems, and Dell Latitude D630 and E6400 laptops. The company also operates approximately 400 PC's and 100 laptops for survey interview processing. The PCs themselves include a wide range of white box desktops, Dell Optiplex desktops, and IBM ThinkPad laptops.

2.8 System Environment and Special Considerations

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.

The IT environment includes local-area networks (switched Ethernet) operating in each of the Company's offices. The LANs also include file servers used for data storage; Novell Netware v. 6.5 is used to provide file and print services. Novell

eDirectory Services is used to authenticate users and provide access to authorized resources.

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.

Secure remote access is provided from PC clients on the Internet to the Company network using VPN technology. The Sonicwall VPN software and firewalls provide 128 bit 3-DES encrypted connections between the remote PC clients and the Company network. User authentication is handled via a user ID and password challenge at the firewall level. Once authenticated, the user can then login to the network to gain access privileges as defined by their eDirectory user profile.

The data center and computer rooms operated within Abt SRBI data collection centers are locked, and have strictly controlled physical access. The Secaucus data center has security staffing 24x7, closed-circuit monitors, secure-card key access, biometrics scanners, man traps, and alarmed doors. Guards maintain access to the loading dock and access requires a card key. The Cambridge computer room, which is shared with Abt Associates, has a secure-card key access. Abt SRBI maintains a 42U data rack within the room and the front door is kept locked at all times.

All on-site network access is challenged and authenticated, with the Novell user ID and password controlling access to the network itself and specific directories and files. Network access is provided only to Abt SRBI employees and designated consultants and subcontractors, under strictly controlled conditions. Application servers (Windows 2003 server running our statistical package, Windows 2003 servers running the Fusion survey products, Redhat ES Linux server running the Quancept survey product, Windows 2003 web servers running the Confirmit Web survey product, Windows 2000 and 2003 servers running the APEX IVR product) have additional, separate user IDs, passwords and user profiles determining logical access.

2.9 Interconnection and Information Sharing

2.9.1 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 Novell Directory Services (eDirectory) or Active Directory.

Connections between the Internet and the Company network are protected by Sonicwalls firewalls, with network controls and protections described in section 4.2.

2.9.2 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.

2.9.3 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.

2.10 Applicable Laws or Regulation Affecting the System

The following laws or regulations apply to the System:

- Privacy Act of 1974 (P.L. 93-579, as amended).
- Freedom of Information Act 1974.
- A client Agency's OMB mandated Data Quality policy.

Depending upon the nature of task orders awarded to Abt SRBI, the following laws and regulations may also apply:

- Health Insurance Portability and Accountability Act of 1996.
- Rehabilitation Act of 1973 (29 U.S.C. sections 794 and 794d, as amended).
- Section 508 of the Workforce Investment Act of 1998 (P.L. 105-220).
- Telecommunications Act of 1996 (P.L.104-104 Feb. 1996, 110 Stats. 56).
- Telecommunications Accessibility Enhancement Act (P.L. 100-542 Oct. 1998).
- Government Information Security Reform Act of 2000 (FY 2001 Defense Authorization Act (P.L.106-398) including Title X, subtitle G, "Government Information Security Reform".
- The IT policy of the Department under which the data are collected, if a finding of "federal interest" is applicable.

2.11 General Description of Information Sensitivity

Because it is a general support system, information stored and processed in the Abt SRBI IT environment ranges from publicly available to highly confidential data, subject to laws and restrictions governing confidentiality, use and access. The requirements below regarding confidentiality, integrity and availability refer to the GSS as a whole; they constitute the minimum set of requirements for information managed as part of a client study or contract.

If applicable, systems, programs and data related to specific contracts/task orders may be subject to the additional requirements of the security plan developed for that contract/task order.

2.11.1 Confidentiality Requirements

Unless a contract/task order involves publicly available data, it is assumed that requirements for confidentiality are MODERATE i.e., data and systems must be protected from access by unauthorized persons; access by unauthorized processes; and unauthorized copying of electronic files.

Failure to preserve the confidentiality of data may be in violation of the law; could compromise the rights to privacy of subjects in research studies; may expose corporate trade secrets; could harm the professional reputation of Abt SRBI and its project sponsors; and could interfere with the ability of Abt SRBI and project sponsors to fulfill their missions.

2.11.2 Integrity Requirements

The work of Abt SRBI relies on accurate processing and analysis of data managed in conjunction with projects/task orders. Therefore, requirements for data integrity are MODERATE. Data must be protected from unauthorized, accidental, unanticipated or unintentional modification.

Inappropriate or erroneous modification of data could compromise the integrity of the analyses performed by Abt SRBI, rendering those analyses and results invalid; could result in managerial or policy decisions to be based upon erroneous data; could harm the professional reputation of Abt SRBI and its project sponsors; and could interfere with the ability of Abt SRBI and project sponsors to fulfill their missions.

A second and potentially more complicated part of integrity has to do with integrity of processes. Assuring the code performs the same way every time; that processes are initiated from trusted environments, access appropriate data, deposit / print results only at approved locations and communicate only with other trusted partners – whether person-initiated or auto-initiated, is included in the overall frame of integrity. In addition, in the distributed (possibly automated) environment, the authenticity of the individual / process is a significant factor, sometimes included under integrity and sometimes identified apart due to its complexity.

2.11.3 Availability

Abt SRBI work and its ability to fulfill its mission are dependent upon the availability and performance of its IT environment. Requirements for availability and good performance of the IT environment are MODERATE. While minor outages (infrequent hours of non-availability) are tolerable, sustained outages are not acceptable.

Sustained non-availability of systems would result in Abt SRBI inability to perform its work and fulfill its mission; it might also result in increased cost to both the Company and government agencies.

3.0 MANAGEMENT CONTROLS

3.1 Applicable Guidance

Abt SRBI policies and standard operating procedures have been heavily influenced by the recommendations made in NIST Special Publications 800-18, *Guide for Developing Security Plans for Information Technology Systems*, 800-12, *An Introduction to Computer Security: The NIST Handbook*, and, 800-14, *Generally Accepted Principals and Practices for Securing Information Technology Systems* as well as guidance provided by IT industry organizations such as the SANS Institute.

Password standards were based, in part, on the Federal Information Processing Standards (FIPS) Publication 112, *Password Usage*, as well as password functionality supported by the systems currently in use.

Policies regarding confidentiality are based on *The Privacy Act of 1974, 5 U.S.C. 552a, As Amended, the Health Insurance Portability and Accountability Act of 1996,* and industry best practices.

3.2 Assignment of Security Responsibility

Primary responsibility for the security of the General Support System (GSS) rests with the Company's Chief Operating Officer (COO). Oversight responsibility for various aspects of GSS security is delegated to the Director of Information Technology and the Manager of Information Technology. Implementation of the GSS security policies and procedures is the responsibility of the Company's network system administrators. Project personnel are responsible for contract-specific security issues outside of the GSS.

3.3 Risk Assessment and Management

3.3.1 Scope of Risk Assessment

IT risk management is focused on any factors which could potentially:

- Materially disrupt the ability of the Company and its staff to effectively use IT resources to perform their work, including regular office automation, communication tasks, and research and consulting work;
- Compromise the confidentiality and integrity of client data collected and maintained by the Company; or
- Compromise the integrity of systems used for internal management purposes.

3.3.2 Risk Factors

In assessing IT risks, the following factors are considered:

- Confidentiality: data are accessed only by authorized users, on a "need to know" basis.
- Security: the IT environment is protected from intrusion, hacking, malicious damage and unauthorized access and use.
- Availability: systems and networks are available during all hours in which Abt SRBI staff work.
- Recoverability: IT resources and data can be recovered reliably and in an acceptable period of time in the event of system failure, data loss or "disaster".
- Maintainability: hardware and software are maintained at appropriate levels of technical currency and maintenance/revision levels, so that all systems receive vendor support have the latest bug patches etc.
- Performance: the IT environment provides the speed and throughput required for efficient processing and data communications
- Functionality: IT resources provide appropriate functional capability to support the Company's client projects and services and internal work.

3.3.3 Risk Evaluation Criteria

Risks to the IT environment are evaluated by considering the following:

- Probability of occurrence, i.e. how likely is it that a given risk event will occur.
- Severity of risk, i.e. what impact would result from the risk event.
- Alternative solutions to mitigate or eliminate risk.
- Cost-benefit and cost-effectiveness of risk mitigation alternatives.
- Impact on operations of risk mitigation alternatives, i.e. does the risk mitigation strategy have an unreasonable negative effect on Company

operations. Typically this assessment involves the tradeoffs between tight security and access/usability.

3.3.4 Risk Assessment Processes

Standard IT risk management processes are included in the IT Standard Operating Procedures Manual. This manual describes our processes for managing risks in the areas of account generation; password control; file access; network security etc.

Each planned change in the IT environment is assessed against the risk factors noted above. New operating procedures and risk mitigation strategies will be developed in accordance with the security planning life cycle described in section 3.5, for all new technologies and services.

3.3.5 External Risk Assessment

Abt SRBI Inc. will conduct an External Risk Assessment in December 2009.

3.4 Rules of Behavior

The rules of behavior outlined here define the terms of use for the Company's Local Area Networks and Wide Area Network, including Internet access and the use of e-mail. Employees will be held accountable for their actions in using the LAN, WAN, Internet access and e-mail. Violations of these rules of behavior may result in disciplinary action at the discretion of corporate management.

3.4.1 Use of the Network

Users are assigned a user ID and password, for purposes of connecting to the Company's network. Users are responsible for the confidentiality of their user ID and password, as well as accountable for their use on the network. User IDs and passwords may not be shared with other users. Employees and other users are expected to behave in a mature and professional manner when using e-mail and accessing the Internet, and to protect the reputation and good name of Abt SRBI when using these systems.

3.4.2 Interconnections

Interconnection to outside autonomous systems or networks is restricted. All such interconnections must be approved by the Director of Information Technology and implemented and managed by the appropriate IT staff, in accordance with the IT Standard Operating Procedures for such connections. The use of unauthorized networking equipment, such as wireless access point, is prohibited.

3.4.3 Telecommuting

All arrangements for working at home must comply with Company policy. The IT department provides equipment, software and network connectivity suitable to support the employee's work and provide secure, encrypted connections to the Company's network.

3.4.4 Dial-in Access

Dial-in access if prohibited and not support at Abt SRBI.

3.4.5 Connecting to the Internet

Some users on the corporate LAN have Internet access. Users are prohibited from transmitting confidential Company or client data in clear text across the public Internet. Users should be aware that their activity on the Internet is logged by the firewalls. Users are expected to use the Internet principally for business purposes; incidental personal use on non-work time is permitted.

3.4.6 Use of Copyrighted Software

LAN and PC users are prohibited from using illegally obtained software on the corporate network and are also prohibited from illegally copying software on the corporate LAN and PC's for other uses.

3.4.7 Misuse of Company Equipment

Network and computer equipment are provided for business purposes. Use of Company equipment for personal gain is prohibited.

3.4.8 Network Access Privileges

Network privileges are given based on a need to perform specific work. Users are required to work within the limits of their access privileges and not attempt to gain access to unauthorized applications or data. Users must never divulge company confidential or client data to unauthorized 3rd parties.

3.5 Planning for Security in the Life Cycle

3.5.1 Overview

All IT equipment and systems have a finite life cycle. The General Support System at Abt SRBI is a complex system with numerous subsystems, all of which require a suitable level of security to ensure reliable operation and the protection of corporate and client data. The general process of integrating security, beginning with needs assessment and finishing with eventual phase-out and disposal, is described below.

3.5.2 Project Request Phase

The introduction of new subsystems or equipment typically begins with the identification of a business need. During the project request phase, IT staff, sometimes in collaboration with project staff, assesses the security requirements of the proposed subsystem, both with regard to data sensitivity and reliability. Managerial approval is required for a proposed project before it proceeds.

3.5.3 Security Specifications

Having identified reliability requirements and potential risks to sensitive data, IT security personnel identify and specify the security requirements for the proposed GSS system, or work in collaboration with project personnel to determine the security requirements for "Major Applications."

3.5.4 Design Review and Test Plan

After initial specification, the security plan is reviewed, and a determination is made as to how security measures will be tested. A design review is conducted, involving both management and IT staff.

3.5.5 Acquisition Specifications

Once the security design has been approved, detailed specifications are prepared to allow the acquisition of the appropriate hardware, software or services. All aspects of the specifications should be described in sufficient detail to allow decision makers to determine if all technical, administrative, physical, and security requirements are satisfied.

3.5.6 Certification/Accreditation

Prior to the new subsystem being introduced into the GSS, sufficient testing, in isolation if possible, will be performed to insure the smooth integration of the subsystem into the General Support System. The new subsystem must be certified by the Manager of Information Technology to validate its reliability and security features. Once certified, the Director of Information Technology must authorize deployment into the GSS.

3.5.7 Implementation Controls

During deployment into the GSS, the planned security measures should be implemented and tested. IT support staff with security and control responsibilities for the technology being introduced will be briefed and trained on the new subsystem.

3.5.8 Operations and Maintenance Controls

Once in production, new subsystems within the GSS are monitored for correct operation, reliability and the effectiveness of the security measures employed. Maintenance to the subsystem is documented and additional training, as needed is provided to IT staff responsible for the subsystem.

3.5.9 Disposal Controls

At the end of the system or equipment life cycle, Abt SRBI IT staff review the security requirements involved in removing equipment and ensure that any sensitive data is thoroughly erased. For example, when file server disk drives containing sensitive data are phased out, the drives are degaussed, reformatted, or pulverized; new file systems created and over-written to erase the former content; magnetic tapes containing sensitive data are either degaussed or shredded. For other equipment or media, appropriate measures are taken to ensure that sensitive data are removed.

3.6 Authorize Processing

The introduction of new systems into the GSS, changes to the GSS, or changes to operational procedures requires management approval. Depending on the extent of the change, authorization might be required of a workgroup manager, a director of a department or the Company's Chief Operating Officer.

3.7 Communications Security

Security measures will be employed that are suitable to the sensitivity of the information being transmitted. If needed, encryption technology ranging from password protected compression for data files to 3DES or AES for data communications will be employed.

3.8 E-Mail/Voice Mail Security

Abt SRBI supports both e-mail and voice mail systems. However, neither system is assumed to be secure or suitable for the transmission of government classified or highly sensitive information.

Both inbound and outbound Internet e-mail streams are scanned for viruses, other malware and spam using FrontBridge Technologies hosted service. This product is licensed on a subscription basis and "signature" updates are provided on a daily basis as part of the subscription entitlement.

In instances where confidential or secret files must be sent via e-mail, commercial packages such as PGP, using 128 or 256 bit encryption, are used to encrypt and sign files for authenticity. When sending material across the Internet, clear text is not advisable. WinZip v10 & 11, one of Abt SRBI desktop tools capable of 256 bit AES

encryption as well as compression, can be used to compress files using a password and the file can be sent as an attachment in a compressed and encrypted format. Both methods require that the recipient possess a password to decrypt the messages, providing both a measure of security and an assurance of authenticity.

3.9 Facsimile Security

The Company supports facsimile (FAX) equipment in all of its offices. However, general-use FAX equipment is not considered suitable for the transmission of classified or highly sensitive information. Some of the Company's FAX equipment is located in areas with restricted access and can be used for transmitting material that is not highly sensitive, but not intended for public access. If contractually required, physically secured FAX equipment will be made available for a project.

4.0 OPERATIONAL CONTROLS

4.1 Personnel Security

4.1.1 Sensitive Positions

All Abt SRBI IT positions have been reviewed for sensitivity and security considerations. Access to various parts of the GSS are restricted based upon the nature and sensitivity level of the position; the nature of the job duties; and the qualifications of the individual employee.

Abt SRBI research and consulting staff work on a wide variety of client projects, accessing data of varying levels of sensitivity. For this reason, all Abt SRBI research positions are treated as potentially sensitive.

4.1.2 Background Screening

To ensure that individuals who join Abt SRBI are well-qualified and have a strong potential to be productive and successful, it is the policy of Human Resources to check the employment references of the selected applicant prior to extending a job offer.

In instances where job responsibilities require access to government classified or highly sensitive data, further background checks are performed as required.

4.1.3 Restricted User Access

User access is restricted to the minimum needed to perform job duties. IT has established minimum default levels of network, e-mail and Internet access for each category of user, including full-time employees, part-time employees, temporary staff, interns, telecommuters, subcontractors and consultants. An appropriate manager must formally request all additional access; the request specifies the specific access needed and its business justification.

4.1.4 User Account Management

IT Standard Operating Procedures Manual specifies formal procedures for requesting, creating, deleting and suspending user accounts.

E-mail and network accounts, with default access to only a personal directory, are established as part of the Abt SRBI hiring process. The Director of Human Resources and SVP's forward the request for new user accounts to the Helpdesk System. Any access beyond the established defaults must indicate the access needed and its business justification. For anyone other than regular staff, the request also includes the start and end date of the account access.

The Manager of Information Technology delegates the task to a network administrator who creates the account with a user ID following a standard Company convention and a default password. The password must be re-set to one of the user's choosing (following Abt SRBI password rules) upon first access to the system. Login and password change instructions are forwarded to the user.

Staff network accounts are closed when an employee terminates, or by request. Abt SRBI has an employee termination process and checklist that serves as a request to disable logins and close system accounts when an employee terminates. Some accounts may also be closed upon request to the Director of Information Technology and the Manager of Information Technology, as when an employee changes duties or job status. User accounts for temporary staff expire automatically on the expiration date set up at account creation, or earlier, as required.

4.1.5 Separation of Duties

Critical functions and the access rights needed to perform them are allocated to staff according to their job duties. In order to minimize the possibility of error or inappropriate use (e.g. fraud), critical duties are separated among staff. For example, staffs who request account creation or access changes are separate from those who can actually perform the request. Similarly, database administrators may not perform system management tasks, and vice versa.

4.1.6 Termination Procedures

For normal, friendly terminations of employment, the Company's Human Resources department has an exit process that includes notifying both the Director of Information Technology and the Manager of Information Technology of the termination. The Manager of Information Technology or a network Administrator, terminate the account at COB on the date requested.

Involuntary or unfriendly terminations always involve Human Resources staff in

the termination process. Where appropriate, HR staff makes special arrangements for account termination, in the form of a request to the Director of Information Technology for special handling of the account termination. In these cases, account access may be terminated immediately or at a specific time indicated by Human Resources or the employee's manager.

4.2 Physical and Environmental Protection

4.2.1 Computer Room Environmental Security

Computer rooms housing file servers, network equipment and other computing hardware are supported in all of Abt SRBI offices. Generally, these computer facilities have dedicated air conditioning, dedicated electrical service, an emergency power panel, Uninterruptible Power Supply (UPS) systems, electrical line conditioning and either biometric hand readers secure-card key access, and or key locks. Some computer rooms supported by Abt SRBI have automated environmental sensors that notify system administrators of abnormal conditions via e-mail or pagers.

4.2.2 Physical Security

Access to the computer rooms is restricted to personnel on an as-needed basis. Entry to our computer room facilities is protected by either biometric hand readers, and or key locks. Our standard operating procedure is to remove privileges, or change the locks, when Information Technology employees with access privileges terminate or change assigned job responsibilities. During a twenty four hour period, our Secaucus data center is monitored by network operations personnel and facilities security staff.

Physical access to Abt SRBI office buildings are restricted by key locks. In addition to the computer rooms, there are some other areas within the buildings, such as data preparation centers, that are restricted by key locks.

4.3 Production, Input/Output Controls

Abt SRBI Survey Operations group supports a data preparation area in our Cambridge office that is secure and accessible only to authorized staff. The area also contains a fire retardant/water resistant safe.

Most printers used for purposes of office automation and data processing are located in employee accessible areas within the Company. Some work groups within the Company operate dedicated printers located in secured areas. To the extent that government classified or highly sensitive information will be printed under any contract/task orders, special arrangements will be made to situate and secure printers in a location accessible only to authorized staff.

4.4 Audit and Variance Detection

Several different types of systems are used within the Company that produces audit trails. The Company's Sonicwall firewalls log all access attempts and connections. The Sonicwalls record both successful and unsuccessful login attempts across the Internet. The Company's Linux server's record logins and detailed command history. Our NetWare 6.5 servers authenticate users through eDirectory, which records failed login attempts and other anomalous user behavior. Computer generated logs are reviewed by or system administration staff on schedules determined by the function of the equipment, the sensitivity of the data stored on the systems, or the likelihood of intrusion attempts.

4.5 Emergency, Contingency Planning and Disaster Recovery

Abt SRBI IT policies and procedures provide for emergency recovery and contingency planning. For example, our network operations staff schedule regular, monitored backups and store the backup tapes off-site. Currently, Abt SRBI maintains 1 year of weekly full backups off-site, and 8 weeks of daily incremental backups on-site. Abt SRBI maintains multiple offices with on-site computer rooms and network connections that could be used as "cold sites" in the event of a disaster. Our Wide Area Network has some redundancy, using a manual fail-over to a VPN encrypted tunnel between sites, if a point-to-point WAN connection fails. In some cases we have unused servers that can be pressed into service in a disaster. In an emergency, backup tapes can be recovered from our off-site storage offices.

4.6 Application Hardware & Software Maintenance Controls

All hardware changes to servers are made by the IT staff responsible for the equipment. Changes are logged in the documentation for the specific server or equipment to provide an historical record.

Software changes, such as operating system upgrades, server application upgrades, etc., are made by the IT staff responsible for the equipment. Changes to application software resident on PC's are also made by the IT staff. The IT staff responsible for desktop application upgrades maintain a log of all changes made and when they occurred.

4.7 Integrity Controls

The Symantec Anti-Virus product is installed on all the desktop, laptop, and some servers used for office automation. Updates to virus signature files are automatically pushed down to the desktops, laptop, and servers during off peak hours or during the login process, allowing an automated process by which anti-viral updates are distributed and installed. This product also performs a scan of the user's PC at every reboot and checks incoming files for virus infection. Warnings of potential virus infection are quarantined and checked by the IT staff on an as-needed basis.

Project data is stored on file servers in directory structures that are protected by system-defined "group" membership, Access Control Lists (ACLs) or user lists. These directories are not accessible by anyone without explicitly defined access privileges.

Network monitoring tools are used to alert the appropriate staff when adverse events occur, such as a switch, router, firewall failure, or a file server crash. Where appropriate, system-monitoring tools are used to analyze performance problems, identify denial of service attacks, or detect a compromised system. In particular, systems exposed to the Internet are hardened and frequently monitored to prevent intrusions.

From time to time, network security staff will perform penetration testing of selected systems to verify system integrity.

4.8 Documentation

Documentation for the GSS consists of both manual and computer generated diagrams of network segments and systems. In addition, activity/change logs are maintained by the system administrators responsible for each major system used in the GSS. IT employees maintain an inventory of systems and network configurations, as well as hardware and software documentation provided by the equipment vendors.

All major systems changes are recorded in the system change log for the system in question. In certain cases, where it might be necessary to replicate systems, our system administrators maintain "how to" instructions for system installation of modifications.

4.9 Security Awareness and Training

Security indoctrination and training occurs at all levels for Information Technology support staff. The Director of Information Technology provides informal training on security issues and practices relating to specific job responsibilities. Security policies and issues are discussed and staff members are asked to provide input in helping to refine security practices to address the issues. Finally, at the IT management level the policy is explained and group responsibilities outlined during department meetings. Project staff workgroups have similar security awareness discussions and training, depending on their job responsibilities and the sensitivity of the data to which they have access. In some cases, project staff members are asked to sign confidentiality agreements before being given access to sensitive data. Project staff working on any government client contract/task order will receive training on the security procedures required by the client, using client-supplied materials if possible.

4.10 Incident Reporting and Response

Abt SRBI IT and project personnel are expected to report any security incidents affecting corporate or client data or systems. Such incidents include system integrity compromises (such as external intrusions or policy breaches such as password sharing), denial of service attempts, compromised security of systems or data, the existence of computer viruses or similar malicious code, and the use of unlicensed commercial software.

All security incidents are sent to the Helpdesk system. The Helpdesk system provides automatic incident tracking and reporting, as well as trouble ticket assignment.

All security incidents are forwarded to the Director of Information Technology and handled with the highest priority and utmost urgency. Depending upon the severity (e.g. Internet hacking, use of unlicensed commercial software), the IT Director will takes steps ranging from correction of the incident, initiating and conducting a security investigation, suspending a particular service, and convening an IT security team to address a critical problem.

Critical systems are monitored for intrusion detection, and regularly tested for potential security weaknesses.

The Manager of Information Technology and the IT staff are responsible for tracking relevant security alerts, advisories and the availability of patches. Typical sources of this information are CERT advisories, the InfoWorld web site, advisories and updates from anti-viral software vendors, national news, and updates from hardware and software vendors.

To the extent that incidents are reported that affect client data or systems, the Director of Information Technology will notify the corresponding client project personnel and attempt to resolve any system security issues. The project personnel in return will notify the client.

5.0 TECHNICAL CONTROLS

5.1 User Identification and Authentication

Each user is assigned a unique user ID and password for access to the corporate LAN. User IDs follow a standard corporate convention. Passwords are a minimum of 8 characters; upper and lower case characters, numerals and special characters are all required for a “strong” password. Users are forced by the system to change their passwords every three months. Some sensitive positions require monthly password changes. Passwords may not be reused within a 2-year window.

Password changes are made by users when password expiration is forced by the system (quarterly or monthly), or more frequently if they so desire. If a password is lost, the user notifies the Helpdesk, who forwards the request for a password re-set to a network administrator. Network administrators issue a new default password for a single login, which the user employs for authentication and then is forced to change after the single use.

If system and network administrators become aware of password compromise, they notify the affected user of the problem, and re-set passwords as described above. Depending upon the circumstances, a security investigation may be launched and appropriate action taken, depending upon the results of the investigation.

The Company uses Novell Directory Services (eDirectory) for network user ID, password and access authentication. All methods of access to the Company network (on-site, Virtual Private Network) authenticate against an LDAP (e.g. eDirectory) server. eDirectory passwords are transmitted in an encrypted form, using RSA 2-way key security. Users are locked out of the system for 15 minutes after 3 failed login attempts. A log entry is created for all lockouts and the content of the log file is reviewed regularly by our network administrators for evidence of possible security breaches. If the lockout is caused by a user's simply forgetting their password, they follow the "lost password" procedure described above.

Authentication may be provided at three different levels, depending upon the services and systems a user is authorized for. As described above, all network access is authenticated using eDirectory. Access to Linux and Windows 2000/2003/2008 servers requires a separate user ID and password, enforced at the operating system level. Finally, certain sensitive applications also require a separate user ID and password, enforced by the application or database management system.

5.2 Authorization Control

Certain applications, e.g. Microsoft SQL, have application-specific access controls to limit data or functional access based on user identity. Abt SRBI corporate policy requires that such privileges be removed when an employee terminates or changes job responsibilities. In addition, access to the systems hosting such applications is typically provided through the corporate network, and depends on having a valid user identity, making these systems inaccessible without a valid network login.

5.3 Logical Access Controls

The types of logical access controls vary by system. Currently there are three kinds of end-user accessible operating systems in use: Novell NetWare 6.5, RedHat ES Linux, and Windows 2000/2003/2008.

NetWare 6.5 controls access to resources, including file system objects, by "context," group membership and user ID. A user's "context" is set when the account is activated. It defines the resources available to the user and disallows

access to resources not within that definition. The “context” is used to restrict user’s access to specific file servers and to the directory structures resident on those servers. In Abt SRBI environment, the user’s “context” restricts the user to the specific file server(s) and directories required by the person’s job responsibilities.

RedHat ES Linux controls access to resources, such as file system objects, based on the user ID, group memberships and Access Control Lists (ACLs). In the Abt SRBI environment, groups are created for projects and project data are typically stored in directories accessible only by members of the group. The default “umask” used to create file system objects give the creator of the file read and write privileges, the group read privileges and everyone else no rights. The creator of the file is able to alter the read/write privileges if needed. In situations where additional security is required within a project, or group, ACLs are used to further refine rights.

Windows 2000/2003/2008 uses file system security similar to that found in Linux, except that in Abt SRBI environment, passwords and ACLs are used as the primary security mechanism. The Windows server systems currently in use have only a small number of users with regular login accounts.

In Abt SRBI environment, most project data reside in directory structures that are protected by either group membership or ACLs. Individuals are given group membership or are included in ACL permissions, based on their job responsibilities. The default profile gives an individual access to their home directories. By default, users have no access to applications, system directories (other than the basics needed for use of shell commands) or other system resources; the typical user might not have access to Linux or Windows server systems, only NetWare.

Requests for additional access privileges for users are sent to the Helpdesk system from Project managers, Group managers or directors. The manager or director who initiates the request is responsible for notifying the Manager of Information Technology when a user job responsibility changes (at which time privileges would be reduced or removed).

User IDs are kept uniform across different platforms where possible. On Linux and Windows server systems, the users are given an initial password and required to change it on their first login, giving them an opportunity to manually synchronize their passwords. The password rules vary across systems, but the general rule for passwords is that there’s a minimum of eight characters in length, not be a dictionary word, and have at least one character that isn’t in the alphabet. On systems that support password rules, the software enforces the acceptability of the password. On other systems, users are given guidelines for password construction. Passwords are set to expire every 3 months and most systems disallow reuse for a 2-year period.

Systems vary in their ability to enforce inactivity logouts. However, the use of a standard screen saver with password protection on PCs used with terminal emulation programs locks the PCs after 15 minutes of inactivity, providing an effective control.

5.4 Network Security

Abt SRBI supports local area networks (LANs) in all eleven 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. In addition, all eleven offices have direct connections to the public Internet. Our Internet connections are protected by Sonicwall firewalls. Internal network security is provided by the use of Novell's Network Directory Services (eDirectory) software, which provides a single user ID, password and privilege profile for the most commonly used network services.

5.4.1 Firewalls

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 performed by the Manager of Information Technology and in cases of significant change, with the approval of the Director of Information Technology.

In those instances where relationships exist with trusted subcontractors, Abt SRBI specifies the security arrangements and our IT staff dictates the firewall policies used on both ends of the connection.

5.4.2 Warning Banner

On initial boot, our desktop and laptop PCs display a cautionary message informing the potential user that the system may be used to perform work for the Federal Government and that usage is restricted. Our network login banner is the generic Novell NetWare client login display. Terms such as "welcome" are not used. In instances where workstations have access to sensitive data, this banner can be supplemented with a restrictive warning suitable to the purpose.

If required by the nature of the work being performed or the sensitivity of the data being accessed, additional warning banners will be displayed, which could include such restrictions as "authorized use only," or "consent to monitoring" messages requiring user acceptance before login.

5.4.3 Network Services

The Company provides only basic network services for office automation for the average user. Additional services or software are made available as needed, on an individual basis, for the fulfillment of job responsibilities. On the Company's NetWare 6.5 file servers, logical access is limited by the user's eDirectory profile.

On other systems with separate logins, such as Linux servers, privileges are limited by login ID, group membership and user profile.

5.4.4 Guest Accounts

"Guest" accounts are not permitted. Each user receives a separate user ID and password, and is responsible for their proper use. Group logins are not allowed. ID and password sharing is prohibited.

The Company operates a standard FTP site, as well as a secure FTP site, for file transfers. No "guest" or "anonymous" accounts are permitted and accounts are created with automatic expiration dates and privileges suitable to the purpose of the account.

5.4.5 Remote Access Security

Telecommuters and other remote access users are allowed to connect to the Company's network. Remote access users can connect using the Sonicwall Virtual Private Network (VPN) client software package over the public Internet. This technology creates a secure tunnel using 3-DES encryption between the user's PC and the Company's firewall. Authentication requires the user's Sonicwall user ID and password.

5.4.6 Internet and Intranet Security

The Company provides limited Internet and Intranet access to employees for business purposes. Typical use includes access to the World Wide Web, Internet e-mail, and occasional file transfers. Our firewalls block most ports, limiting access only to a subset of the standard TCP/IP protocols. Depending on business requirements, arrangements can be made for special firewall rules to allow other types of access. Special firewall rules are provided only after a security evaluation by the Manager of Information Technology and with the approval of the Director of Information Technology.

5.4.7 Web Site Operations

Abt SRBI operates a number of web sites, both for internal purposes and for dissemination of project information. To the extent that any awarded task orders require web sites, the operating principle will be to provide maximum availability at acceptable levels of risk.

Access and security controls will be deployed that are suitable to the level of risk. Web sites must be hosted behind firewalls, have application security controls where applicable and be subjected to penetration testing as part of the acceptance procedures. Each web site will have a suitable security plan, including appropriate contingency and disaster recovery plans.

5.5 Workstation and Desktop Security

The Company supports approximately 150 personal computers (PC's) connected to the corporate LANs. These PCs are used for office automation, data entry, statistical analysis and data communications. Company policy requires that all sensitive or business critical data sets reside on central file servers, where access control can be centrally maintained. The Company's IT organization provides password-protected screen savers for desktop PC's, to protect against unauthorized access. PCs used to access sensitive or confidential data will be secured in a manner commensurate with the level of risk

5.6 Audit Trails and Journaling

To the extent that commercial data base systems, such as Microsoft SQL, will be used for awarded tasks, applications will be designed, if needed, to create and use transaction logs to allow rollback or reconstruction of files.

Some of the Company's manual and automated processes performed by data preparation or data entry personnel are monitored by paper or automated audit trails, and in some cases, changes are recorded in a separate journal file. Depending on the nature of the tasks awarded, such techniques might be employed in the completion of the work.

5.7 Confidentiality Controls

All client data, unless specifically intended as "public use" or in the public domain, are treated as confidential. Data of a sensitive nature sent to or from a client site should be transported by a secure carrier or transmitted in an encrypted state. In particular, Company policy requires that no highly sensitive client data should be sent in "clear text" across the public Internet.

Sensitive client data stored on computers owned or operated by Abt SRBI will be protected by mechanisms appropriate to the level of risk. Some techniques currently in use include storing data in system directories protected by group membership access, special passwords, encryption, physically secure isolation of systems, or a combination of these.

Requests made to Abt SRBI under the Freedom of Information Act will be forwarded to the client for action.

6.0 Additional Comments

Abt SRBI Inc. has a long history of protecting the confidentiality of data. For over twenty five years, we have conducted numerous research studies involving sensitive information; consequently, facilities and procedures have been developed to maintain this confidentiality. Our Cambridge, MA office was approved for paper handling. Access to the data processing areas is controlled, with only authorized personnel allowed in the computer rooms, data preparation areas and the computer tape libraries. Locked tape files and storage areas are available for use by all contracts. In addition, project directories and databases are protected by assigned group memberships, passwords and other techniques (e.g. ACLs) that prohibit access by unauthorized users. Building security forces are on duty 24 hours, seven days per week at some of our offices. Access to areas where confidential data are maintained is restricted to authorized personnel.

Abt SRBI Web, IVR, 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.

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.

The procedures currently used within the Company have proved sufficient to ensure the privacy and security of Abt SRBI many research databases.