ATTACHMENT 2:
NETWORK SECURITY AT RTI INTERNATIONAL

Warning: This document should be considered sensitive. Limit distribution to an as-needed basis.

Introduction

This document presents information on RTI International's (RTI) Information Technology (IT) Security for the Screening, Brief Intervention and Referral and Treatment's (SBIRT) III evaluation.

Security Regulatory Requirements

In recognition of the importance of the security in privacy of client data, RTI has designated IT Security and Privacy Offices to review and ensure compliance with current federal regulations, guidelines, and client requirements. RTI's information systems professionals pride themselves on their knowledge of established federal information security requirements—such as the Health Insurance Portability and Accountability Act (HIPAA) and the Privacy Act of 1974—and on staying constantly abreast of all new requirements, including the 2002 Federal Information Security Management Act (FISMA) and the 2002 Confidential Information Protection and Statistical Efficiency Act (CIPSEA).

These laws require that private enterprises providing service to the government meet these same standards. Therefore, RTI has voluntarily and enthusiastically embraced the IT security guidelines and principles published by the National Institute of Standards and Technology (NIST). Using the formulas provided by NIST, RTI staff determine which level of security is required and implement either RTI's Standard Security Infrastructure (for data defined by Federal Information Processing Standards [FIPS 199, as low potential impact) or RTI's Enhanced Security Infrastructure (for data defined by FIPS 199 as Moderate potential impact).

The requirements to implement IT security for research projects at the more rigorous FIPS 199 moderate level are currently beyond the capabilities of many corporations, universities, and other research organizations. Therefore, these organizations might be genuinely unaware of the significant legal implications of security requirements and/or may fail to address them adequately in contract proposals and work plans. RTI has distinguished itself by creating a self-contained Enhanced Security Network (ESN), which is certified and accredited at the FIPS 199 moderate level for both confidentiality and integrity. The ESN forms a dedicated network segment within the confines of the RTI corporate network and employs a highly restrictive set of IT security controls, allowing it to compliantly host project systems requiring protection at the NIST moderate level.

With RTI's resources and attention to security policy, we can recognize those project systems or subsystems that will legally require IT security at moderate (versus low) levels, as mandated by federal regulations, and provide NIST-compliant IT security for project systems and subsystems that require the more rigorous FIPS 199 moderate designation.

These capabilities elevate RTI apart from other shops in both the private sector and academia. RTI can provide solid advice, backed up by the advanced IT security infrastructure needed to effectively comply with federal IT and data security laws.

Both RTI's corporate and Internet-accessible Standard Security Infrastructures have been certified and accredited and received an Authority to Operate in accordance with NIST special publication 800-37

(Guide for the Security Certification and Accreditation of Federal Information Systems). Criteria for compliance with the newly implemented FISMA regulations, as specified by NIST 800-37, can vary from project to project, and even among subtasks and add-ons within a project, depending on the type of data. For this reason, RTI maintains a staff of IT security and privacy professionals with expertise on these criteria who can quickly evaluate client needs and use RTI's considerable resources to develop and implement an appropriate system security plan according to the nine steps outlined by NIST:

1. Categorize the information to be protected.
2. Select minimum baseline controls.
3. Refine controls using a risk assessment procedure.
4. Document the controls in the system security plan.
5. Implement security controls in appropriate information systems.
6. Assess the effectiveness of the security controls once they have been implemented.
7. Determine agency-level risk to the mission or business case.
8. Authorize the information systems for processing.
9. Monitor the security controls on a continuous basis.

The success of the resulting information system is measured according to three security objectives: confidentiality, integrity, and availability. While meeting and exceeding baseline security controls for both moderate- and low-impact systems, RTI ensures that each of these three objectives is fulfilled without sacrificing the others.

Security Controls

The following are control families from NIST SP 800-53 Rev 3 in which RTI will ensure that our clients' data security systems meet or exceed requirements set by federal law:

- **Access control**. RTI takes steps to limit information system access to authorized users, to processes acting on behalf of authorized users or devices (including other information systems), and to types of transactions and functions that authorized users are permitted to exercise.
- **Audit and accountability**. RTI creates, protects, and retains information system audit records that are needed for the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity, ensuring that the actions of individual users can be traced so they can be held accountable for their actions.
- **Awareness and training**. RTI ensures that managers and users of information systems are made aware of the security risks associated with their activities and of applicable laws, policies, and procedures related to security and that personnel are trained to carry out their assigned information security-related duties. All RTI staff are required to take annual IT security awareness training.
- **Certification, accreditation, and security assessments**. RTI assesses security controls for effectiveness, implementing plans to correct deficiencies and to reduce vulnerabilities, authorizing the operation of information systems and system connections, and monitoring system security controls. This program is managed by a trained Information Security Officer.
- **Configuration management**. RTI establishes baseline configurations and inventories of systems, enforces security configuration settings for products, and monitors and controls changes to baseline configurations and to components of systems throughout their system development life cycles.
- **Contingency planning**. RTI establishes and implements plans for emergency response, backup operations, and post-disaster recovery of information systems.

- **Identification and authentication**. RTI identifies and authenticates the identities of users, processes, or devices that require access to information systems.
- **Incident response**. RTI establishes operational incident handling capabilities for information systems and for tracking, documenting, and reporting incidents that could pose a threat to the integrity, availability, or confidentiality of RTI resources.
- **Maintenance**. RTI performs periodic and timely maintenance of systems and provides effective controls on the tools, techniques, mechanisms, and personnel who perform system maintenance.
- **Media protection**. RTI protects information in printed form and on digital media, limiting access to information to authorized users and sanitizing or destroying digital media before disposal or reuse and providing training to staff on the proper handling of printed media.
- **Personnel security**. RTI ensures that individuals in positions of authority are trustworthy and meet security criteria, ensures that information and information systems are protected during personnel actions, and employs formal sanctions for personnel failing to comply with security policies and procedures.
- **Physical and environmental protection**. RTI limits physical access to systems and to equipment to authorized individuals, protects the physical plant and support infrastructure for systems, provides supporting utilities for systems, protects systems against environmental hazards, and provides environmental controls in facilities that contain systems.
- **Planning**. RTI develops, documents, updates, and implements security plans for systems.
- **Risk assessment**. RTI assesses the risk to organizational operations, assets, and individuals resulting from the operation of information systems and the processing, storage, or transmission of information.
- **Systems and services acquisition**. RTI allocates resources to protect systems, employs system development life cycles processes, employs software usage and installation restrictions, and ensures that third-party providers employ adequate security measures to protect outsourced information, applications, or services.
- **System and communications protection**. RTI monitors, controls, and protects communications at external and internal boundaries of information systems and employs architectural designs, software development techniques, and systems engineering principles. To promote effective security, RTI has implemented an information security program based on the Defense in Depth concept, which combines the capabilities of people, operations, and technology. The IT Security staff maintain several professional certifications, including Certified Information Systems Security Professional (CISSP) and firewall vendor certifications.
- **System and information integrity**. RTI identifies, reports, and corrects information and system flaws in a timely manner, providing protection from malicious code and monitoring system security alerts and advisories.

RTI places great importance on maintaining the highest standards of confidentiality, integrity, and availability for our clients' data. Through our experience with and our proactive approach to these regulations, RTI is able to draft and enact an information security plan and offer premium data security and protect our federal clients from the liabilities that can result from noncompliance.

Computing Infrastructure

All analytic and reporting activities are executed on RTI's corporate computing infrastructure, which is available only to properly qualified and credentialed RTI employees and which is securely isolated from the public Internet.

Data are stored on secure file servers that are backed up nightly and isolated from the Internet by the RTI corporate firewall. Secure data storage is accessible to offsite RTI employees and other properly authorized designees via an encrypted virtual private network (VPN). Programmers, analysts, IT staff, and management staff access data sets and reports on file servers from their desktop computers, which are connected to the corporate network via 1 Gigabit/sec Ethernet networking.

The servers themselves reside in a secure, locked server room, which is accessible only to properly authorized IT staff. Servers and desktops run Microsoft Windows family operating systems, and user access to network resources is password protected through domain-level logins. RTI servers employ a variety of security measures, including antivirus software and secure socket layer encryption.

Technical

The following section provides information on the key processing elements being arranged with RTI Information Technology Services (ITS). RTI's computing infrastructure is well equipped to provide the processor speed and disk storage required for this project. Also, every username on all RTI systems has an associated strong password.

In addition, the project team is addressing the handling of physical media to keep it secure. RTI ITS will supply the bandwidth, encryption, and protocols for telecommunications. The project team is also currently addressing software to be used for system development (programming languages, CASE tools, version control, and configuration control) and operational platform tools (e.g., server, workstation and Web operating systems, database engines).

Hardware

The data acquisition and processing system uses standard RTI hardware platforms and off-the-shelf software similar to that described in Table 1:

Table 1. Standard Hardware Platforms and Software

System Component	Hardware Platform	Operating System	Software
Desktop Workstations for Project Staff	RTI Standard Desktop Class Computer	Windows 7	SAS, Visual Studio.NET, Microsoft Office , Excel, Access, Erwin, SAS ETL, SQL, PowerBuilder, Visual Basic
Laptops	Lenovo X250	Windows 7	Microsoft Office Suite, Microsoft Outlook Express, Stata
Electronic Mail Servers	Dell Servers	Microsoft Windows Server Family	Microsoft Exchange Server, POP3/SMTP Mail Servers
Database Servers	Dell Servers	Microsoft Windows Server Family	Microsoft SQL Server, Oracle
Network File Storage	EMC Storage Processors and Storage Area Network (SAN) Technology	N/A	N/A
Corporate Network	Cisco-based 100 Mb to-the-desktop switched Ethernet Network	N/A	N/A

Resources and Expertise

The SBIRT data acquisition and processing operations are headquartered at RTI's main facility in Research Triangle Park (RTP), North Carolina. RTI provides an in-house team of analysts and programmers who have understanding, detailed knowledge, and long-running experience with many of SAMHSA's key data sets, including the National Survey on Drug Use and Health (NSDUH), the National Survey of Substance Abuse Treatment Services (N-SSATS), the Treatment Episode Data Set (TEDS), and the Drug Abuse Warning Network (DAWN). RTI also has extensive experience in study design, sampling, estimation, preparation and management of analytic files, data analysis, statistical table production, and publication of reports.

In addition, RTI also practices physical security where our facilities, personnel, and equipment and documentation are concerned. RTI has in place standard operating procedures (SOPs) and RTI policies that ensure that only authorized personnel can access RTI offices, and that all our staff are trained to keep data confidential and secure at all times. In addition, our System Security Plans (SSPs) address physical and environmental protections and personnel training and vetting. Finally, RTI's Corporate Security ensures that the facilities are monitored 24 hours a day, 7 days a week.

One of the keys to our data security is having the core of RTI's Local Area Network (LAN) located in multiple RTI Data Centers. This ensures that the same level of physical security, electrical power conditioning, environmental conditioning, and monitoring is provided to the network equipment as to the servers. The network is automatically monitored for utilization and faults, and on-call staff receive automatic e-mail and pager notifications if a problem is detected.

RTI maintains several fully switched and routed Ethernet-based LANs to support both corporate and project initiatives. RTI wide area networks (WANs) employ technologies that include site-to-site VPN, Metro Ethernet, MPLS, VSAT, Voice over IP (VoIP), and WAN Acceleration appliances.

RTI maintains security by providing remote access to the data networks through client-computer-installed virtual private network (VPN) software and clientless secure sockets layer VPN (SSL/VPN) portal. Only authorized staff can access RTI's network from the Internet, and access is controlled by RTI's Internet firewalls. RTI also requires the use of Digipass two-factor authentication for remote access.

RTI maintains two links to the Internet: a primary 1 Gb fiber link and a secondary 100 Mb/sec microwave link. RTI's Internet service provider links are path-diverse and terminate in separate data centers on RTI's main campus. Both links are maintained in an active state and configured for automated, unattended failover.

RTI Operations

RTI's responsibilities include data analysis and storage of analytic data files. RTI's data processing involves storing source and result data sets, creating new and intermediate analytic data sets, and generating reports. All data storage and analysis activities are performed entirely on RTI's secure corporate network.

RTI's Information Technology Services (ITS) supports RTI's voice, video, and information systems and network. Systems are available and monitored 24 hours a day, 7 days a week. Significant investments have been made to ensure the systems maintain an extremely high level of availability and reliability in support of the campus and global networks. This includes, but is not limited to, redundant power systems, virtual private network (VPN) and redundant networking technologies, load balancing devices, clustering, and multiple data centers.

The RTI data network is a fully switched Ethernet-based network interconnecting all buildings on RTI's main campus as well as several remote locations, including our Washington, D.C. offices. Regional offices are connected to the network via dedicated network circuits or via the Internet using VPN technology.

RTI will use its data network and IT infrastructure as described below, and will ensure computer and network security by following NIST standards. Equipment used in the field (PCs) will be configured to maintain the highest security possible. In addition, the project will use RTI's infrastructure to ensure that routine operations are carried out.

Data Network and IT Infrastructure

The core of the RTI Local Area Network is located in the RTI Data Centers to ensure the same level of physical security, electrical power conditioning, environmental conditioning, and monitoring is provided to the network equipment as is provided to the servers. Web content delivery is provided using multiple highly available FIPS 140-2 compliant hardware load-balancers. The network is automatically monitored for utilization and faults. Notifications are sent via e-mail and SMS messaging to the on-call staff if a problem is detected.

All SBIRT data stored on RTI network storage devices are isolated and protected from the Internet by RTI's corporate Internet firewall, which is RTI's first and most effective line of defense and provides effective isolation of the RTI corporate network. The SBIRT data and associated information resources are further secured using a comprehensive set of internal security controls. A multilayered antivirus program is in place. Computer-based tools are used to detect and identify vulnerabilities on RTI systems. Alerts are sent 24 hours a day, 7 days a week via e-mail and pager to on-call staff for evaluation and resolution.

Every business day, a differential backup is created of all new or modified files. Tapes from complete backups are kept for approximately 3 months. Tapes or CDs are used for long-term data archiving. The tapes from the current complete backup are stored in the computer room for easy access. The tapes from the previous backup set are stored off-site. This procedure ensures data availability in the event of a catastrophic event in the computer room. The SBIRT Information System Security Plan will provide a more complete description of RTI's computer security controls and procedures. In addition, RTI has a Business Continuity Plan (BCP) that addresses recovering its data processing and system capability in the event of an emergency or disaster situation.

Subcontractors

All subcontractors working on this project will follow protocols developed by RTI and any others necessary to ensure data security. RTI produces and delivers reports and data to SAMHSA in a variety of formats, including electronic documents via e-mail, hard copy, fax, and CD/DVD. RTI also receives data and associated files/documentation from CSAT/SAMHSA, and others. Typically, this receipt is done using e-mail, FTP, or by physical delivery of CD/DVD storage media. All cogent protocols will be followed for each format to ensure secure delivery and receipt.