ATTACHMENT 9:
NETWORK SECURITY AT RTI INTERNATIONAL

RTI International (RTI) has implemented an Information Security program based on the Defense in Depth concept. This strategy combines the capabilities of people, operations, and technology. Some of the key highlights of this security system are as follows:

- The first layer of protection is RTI's Internet firewall, which connects RTI to the Internet. All traffic between the RTI network and the Internet passes through this single connection point, providing the same level of protection and monitoring to all systems connected to or accessing the RTI network.

- The firewall is programmed with a set of rules to determine if network access is in compliance with RTI's network security policy and then allow or prevent access to the RTI network. The firewall logs all incoming traffic from the Internet to the RTI network. This information is essential in detecting and analyzing any problems.

- The firewall is used to create two RTI networks with different levels of access from the Internet. These networks are called the "private network" and the "public network." The private network is the main RTI network, and most systems are located on it. Access to this network from the Internet is very limited, using a limited set of protocols into specific systems. For example, incoming electronic mail is only permitted to specific mail servers. The public network is more accessible from the Internet and is where World Wide Web servers, anonymous FTP servers, and other publicly available systems are located. Servers on the public network must be registered with Information Technology Services (ITS) and must specify which services they run. This enables the firewall rules to allow only those services required. By not allowing unnecessary services, the overall security of the public servers is improved.

- Web servers are placed behind load balancing devices, which are configured to deny all traffic not specifically allowed according to their configuration. This serves as a layer of protection between the network connecting the Web servers and the public network. Only approved file types are allowed on the Web servers. For example, CGI scripts are not permitted on Web servers.

- Computer-based tools are used to detect and identify vulnerabilities on RTI systems. This ensures that vulnerabilities, if detected, can be corrected before unauthorized persons exploit them.

- Multiple layers of automated network and server monitoring quickly identify failures or unusual activity levels, which may be an indication of an attempted security breach. Alerts are sent 24 hours a day, 7 days a week, via e-mail and pager to on-call staff for evaluation and resolution.

- System and network administrators are automatically subscribed to multiple mailing lists to ensure that they are quickly informed of security advisories. This includes CERT, Microsoft, Network Associates, Trend Micro, and SANS. RTI is an active member in InfraGard, a cooperative security program between the FBI and commercial enterprises.

- A multilayered antivirus program is in place. All e-mail is scanned. Antispam filters are in place.

- Security awareness articles are posted on the internal RTI Web site several times a year to ensure that staff remain aware and vigilant about following appropriate security precautions.

- The Director of IT Security maintains an active Certified Information Systems Security Professional (CISSP) certification. The firewall administrator has been certified as an administrator by the firewall vendor.

RTI Field Laptop Data Security

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

Introduction

This document describes software security practices regarding field laptops, including data and data transmission, for projects using RTI's integrated field management system.

1 RTI In-House Systems

All data are stored behind RTI's firewall on project shares with limited access.

2 Laptops

2.1 Passwords

Laptop users must provide separate passwords to access the laptop, applications on the laptop, and RTI networks. Laptop systems internally supply passwords to FTP sites and RTI database servers.

2.2 Data

2.2.1 CAI databases

Case data are stored in files or databases according to the CAI software used. These include SQL Server, Blaise, CASES, custom software, and other third party software. The security of the files or databases is based on password protection of laptop access.

2.2.2 CAI data for transport

Cases are exported as final or as the result of a transfer. Typically they are extracted from the CAI database and zipped. These files are sent via FTP to RTI.

2.2.3 Case deletion and backup

Finalized or transferred cases are deleted from laptops. An in-house copy must be validated before deleting from laptops. Finalized cases are validated as having been received intact according to project specific rules. Transferred case zip files must be validated as containing the correct files according to project specific rules. Deletions are delayed at least 24 hours to allow for tape backup of the validated in-house copy.

2.3 Data Transmission

2.3.1 Connections

Data transmissions are fully scripted and non-interactive; once the connection is made, the software performs all its activities and then terminates the telephone connection. Connections are via dialup or broadband. Dialup is direct to RTI servers. With broadband, a router is used with firewall enabled (With broadband, wireless connections are disabled on the laptop).

2.3.2 File transfer

Files are transferred via normal FTP, without automated encryption. In combination with dialup, they are transmitted over the telephone line. Using broadband, they are transmitted over the Internet.

2.3.3 Status code updates, events, ePTE, logging, etc.

2.3.3.1 Dialup and direct database server connections

- Transmitted in the clear over the telephone line

2.3.3.2 Dialup and Web service

- Transmitted over https (secure sockets) over telephone lines

2.3.3.3 Broadband and Web service

- Transmitted over https (secure sockets) over the Internet

2.4 Laptop access to Web site

Supervisor laptops often have Internet access in order to use the IFMS or other Web sites. Dialup to local ISP numbers is often used. Broadband connections are also used. Web sites are password-protected.

2.5 Other laptop policies

Use of RTI pool laptops on home wireless networks is not permitted.
Upon receipt of pool laptops, field staff must sign a document stating they will not alter its configuration.