

# **Security Considerations in Implementing MultiSpeak®-Compliant Applications**

Prepared by:

Cornice Engineering, Inc.  
P.O. Box 2350  
Pagosa Springs, Colorado 81147

For:

National Rural Electric Cooperative Association  
4301 Wilson Boulevard  
Arlington, Virginia 22203

February, 2005

Copyright © 2005 by National Rural Electric Cooperative Association.  
All rights reserved. Reproduction in whole or in part is strictly prohibited without prior written approval of the National Rural Electric Cooperative Association. NRECA grants its members and MultiSpeak member companies permission to make copies of this document for their internal use.

### **Legal Notice**

WHILE THE INFORMATION IN THIS PUBLICATION IS BELIEVED TO BE ACCURATE, NEITHER NRECA NOR CORNICE ENGINEERING, INC. MAKE ANY REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, WITH REGARD TO THIS MATERIAL INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. NEITHER NRECA NOR CORNICE ENGINEERING, INC. SHALL BE LIABLE FOR ERRORS CONTAINED HEREIN OR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE OR USE OF THIS MATERIAL. THE INFORMATION CONTAINED IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE.

---

## Table of Contents

---

Section		Page
	<b>Table of Contents</b>	iii
<b>1.0</b>	<b>Introduction</b>	1-1
1.1	Purpose of This Document	1-1
1.2	The Need for Security	1-1
1.3	Design of MultiSpeak Communications	1-3
1.4	Cautions When Implementing MultiSpeak	1-4
1.5	How MultiSpeak Security Fits Into an Overall IT Security Plan	1-5
1.6	On-Going Security Developments	1-6
<b>2.0</b>	<b>Specific Risks and Countermeasures</b>	2-1
2.1	Data System Security Services	2-1
2.2	Threats to MultiSpeak Data Messages	2-1
2.3	Approach to Provide Secure MultiSpeak Communications	2-3
2.4	Optimizing the Performance of Secured Applications	2-5
<b>3.0</b>	<b>Recommendations</b>	3-1
<b>4.0</b>	<b>Glossary</b>	4-1
<b>5.0</b>	<b>References</b>	5-1

# 1 Introduction

- 1.1 Purpose of This Document
- 1.2 The Need for Security
- 1.3 Design of MultiSpeak Communications
- 1.4 Cautions When Implementing MultiSpeak
- 1.5 How MultiSpeak Security Fits Into an Overall IT Security Plan
- 1.6 On-Going Security Developments

## 1.1 Purpose of This Document

Cooperatives, as with all industries, are finding significant advances in productivity by improving the integration of software applications. The MultiSpeak Initiative has played a central role in this process by defining standard data interfaces and ways that those interfaces can be implemented. As cooperatives continue to implement MultiSpeak-compliant software, it is appropriate that they also use the opportunity to critically examine some key aspects of their overall information technology (IT) security. These security issues have always been present in cooperative operations, but come to the forefront with the emergence of MultiSpeak and other rapidly evolving changes to the IT environment.

The purpose of this document is to highlight some of the IT security issues that are specifically related to data exchange and interoperability of application software. This document also outlines for the utility staff member how data exchanged using MultiSpeak messages may be secured.

**It is important to realize that services that are implemented to enhance the security of MultiSpeak messages do *not* constitute a comprehensive approach to cyber-security. Complete security can only be ensured by implementing a comprehensive security policy. The approaches discussed in this document will only be effective when applied in the context of a comprehensive security framework.**

## 1.2 The Need for Security

The key to managing information securely is finding an appropriate balance between providing the data access necessary for efficient operations and, on the other hand, controlling access to sensitive information and protecting critical infrastructure.

Many trends in the electric utility industry have increased the importance of adequate cyber security. Among these are:

- **Increased reliance on information technology (IT) to enhance employee productivity.** In recent years, utilities have implemented systems to increase employee productivity and reduce response time in outage situations. Often such systems have relied on remote access to data and/or the ability to remotely control operational systems. This trend has reduced the security of some systems.
- **Improved integration among utility IT systems.** Increasingly utilities are integrating IT systems in order to gain business process improvements and minimize duplicated effort. Any action that enhances access to, and/or integration of, systems inherently increases the risk of malicious access to data resources. Inherent in any discussion of system integration should be the consideration of data access control.
- **Increasing use of computer networks to ease access to information within the company; and use of the wider Internet to enhance information exchange with resources outside the company's network.** For example, the easy availability of connectivity over the Internet has led to increased use of the Internet infrastructure as part of utilities' wide area networks.
- **Increased reliance on open-source data exchange protocols.** The application of interconnected networks has been facilitated by standard data exchange protocols, such as TCP/IP. However, greater access to data on corporate networks or on the wider Internet, and a greater reliance on standard data protocols leads to substantially increased potential for malicious access to sensitive corporate data.
- **Increased use of real-time systems.** Many of the real-time systems currently in place in utilities were not designed with cyber-security in mind. This shortcoming is amplified when such real-time systems are connected to a trusted business computer network. In many cases, security cannot be added after-the-fact on existing systems since the performance of operational control systems, such as SCADA systems, could be unacceptably degraded if significant security countermeasures were adopted. It is especially important that utilities investigate the risks associated with such systems and investigate with their software vendors potential countermeasures that will not degrade the system's ability to serve its primary goal.
- **Increased emphasis on protecting critical infrastructure from potential terrorists.** Since September 11, 2001, utilities and federal regulators have become increasingly aware of the potential for terrorist attacks on critical infrastructure, such as facilities of electric utilities. It is widely believed that

the ability of terrorist organizations to mount effective cyber warfare is maturing.

- **Increased threats to IT resources from malicious attacks, either by hackers or by disgruntled insiders.** Anyone associated with IT knows about the accelerating rate of malicious attacks on computerized systems. Some studies estimate that the frequency of attacks on critical IT infrastructure has increased by 400 percent during the 1999-2002 period [DHS, 2003, pg. 10]. The tendency is to protect from threats from outside the trusted network which is appropriate. However, often overlooked is that the majority of successful attacks generally come from disgruntled insiders: ex-employees, contractors or ex-employees of vendors. Cyber security plans should not presume that attacks will come from outside the utility's trusted network.

Perfect security can only be achieved in a system that does not provide access to any data or permit any control action to be taken; clearly an unacceptable situation. Also unacceptable, is past practice that relied on proprietary database structures or obscure data protocols; so-called *security by obscurity*. Its underlying assumption that few people would have the knowledge to fraudulently obtain or modify data in such a system has never provided good access control. With modern standardized databases and open-access data protocols, this has become a totally unacceptable means to provide IT security.

### 1.3 Design of MultiSpeak Communications

The MultiSpeak Initiative has defined standard interfaces to support common utility business processes [MultiSpeak, 2003a] and issued recommended practice documents [MultiSpeak, 2003b, c, d and 2004a] outlining ways that MultiSpeak interfaces may be implemented. A document [MultiSpeak, 2004b], targeted primarily to vendors, suggesting how data exchanged using MultiSpeak interfaces may be secured has also been issued.

MultiSpeak messages may be exchanged using a variety of communications transports, including file-based (so-called *batch*) transfers, Simple Object Access Protocol (SOAP) messages, TCP/IP socket streams, and web services. The data sent are identical, regardless of the transport chosen. Only the messaging components change between transmission methods. All of these mechanisms rely on the transmission of data sent as extensible markup language (XML) along with messaging components that are also formatted as text. It is assumed that, with the possible exception of batch file transfers, all of the transport mechanisms rely on TCP/IP networking.

## 1.4 Cautions When Implementing MultiSpeak

It is important for the utility staff member to recognize that one of the principal advantages of MultiSpeak - well-defined standardized data exchanges using common network protocols - may lead to potential security risks, specifically:

- The specification is openly available from the MultiSpeak web site.
- Acceptable message structures are clearly identified in the specification.
- MultiSpeak messages are typically sent over standard TCP/IP networks, which are well understood by potential attackers.
- Real-time communications using either SOAP or web services transports are typically carried over TCP/IP Port 80, a port that is often left unblocked in utility firewalls so that access to web pages is possible by staff members.
- There is no inherent way to determine whether a MultiSpeak message originates from within or outside the utility's trusted computer network.
- MultiSpeak has been designed to support communications within the cooperative and between the cooperative and its business partners, thus opening up the number of communications channels and increasing the number of persons with access to the information.
- Security is **not** specifically required in the MultiSpeak specification in order for commercial software to be deemed MultiSpeak-compliant.

***As a result, it cannot be assumed that an unsecured MultiSpeak message is trustworthy.***

Since layering security on MultiSpeak data messages increases message size and may deteriorate application performance, it is up to the utility to work with its vendors to determine when the application of security is warranted. The purpose of this document is to recommend the approach that should be implemented when MultiSpeak messaging security is deemed appropriate.

All of these characteristics mean that the staff member concerned with implementing MultiSpeak data exchanges or the utility's security policy should carefully consider the potential security risks of MultiSpeak messaging and adopt appropriate countermeasures.

This is **not** to say that you shouldn't use MultiSpeak. Any form of integration will have its own risks and most will be at least as risky as MultiSpeak, only without the associated benefits of standardized data exchanges. Furthermore, the use of MultiSpeak should simplify adoption of countermeasures by bringing together vendors to support a common security approach.

***The important point is that you need to implement MultiSpeak in the context of a comprehensive IT security plan.***

## 1.5 How MultiSpeak Security Fits Into an Overall IT Security Plan

The sidebar below outlines the approach to security assessment and risk mitigation suggested by the North American Electricity Reliability Council (NERC). NERC recommends that (i) such steps be taken during the development of a utility's cyber security plan and (ii) the utility document required actions and procedures in the form of a security policy.

### **Risk Assessment Methodology**

The North American Electric Reliability Council (NERC) has issued a set of recommendations, *Security Guidelines for the Electricity Sector* [NERC, 2002]. As part of the section in that document on Vulnerability and Risk Assessment, it suggests that utilities consider the following steps:

#### **1) Identification of assets and loss impacts**

- a) Determine the critical assets that require protection.
- b) Identify possible undesirable events and their impacts.
- c) Prioritize the assets based on consequence of loss.

#### **2) Identification and analysis of vulnerabilities**

- a) Identify potential vulnerabilities related to specific assets or undesirable events.
- b) Identify existing countermeasures and their level of effectiveness in reducing vulnerabilities.
- c) Estimate the degree of vulnerability relative to each asset.

#### **3) Assessment of risk and the determination of priorities for the protection of critical assets**

- a) Estimate the degree of impact relative to each critical asset.
- b) Estimate the likelihood of an attack by a potential adversary.
- c) Estimate the likelihood that a specific vulnerability will be exploited.
- d) Prioritize risks based on an integrated approach.

#### **4) Identification of countermeasures, their costs and trade-offs**

- a) Identify potential countermeasures to reduce vulnerabilities.
- b) Estimate the cost of the countermeasures.
- c) Conduct a cost-benefit and trade-off analysis.
- d) Prioritize options and recommendations for senior management.

The information presented in this document is intended to assist the utility staff member in completing the following steps in the NERC procedure:

**2a) Identify potential vulnerabilities related to specific assets or undesirable events.** Section 2.2, Threats to MultiSpeak Data Messages, includes a discussion of vulnerabilities of the utility IT systems that could be integrated using MultiSpeak data exchanges.

**4a) Identify potential countermeasures to reduce vulnerabilities.** Section 2.3, Approach to Provide Secure MultiSpeak Communications, outlines the suggested countermeasures to adopt when action is called for by the utility's security plan.

**4c) Conduct a cost-benefit and trade-off analysis.** Section 2.4, Optimizing the Performance of Secured Applications, discusses balancing the security risks with the potential impact on the operation of utility computerized systems resulting from adoption of the countermeasures discussed in this document.

Additional information about completing a utility security plan may be found in the handbook entitled *Information Technology Security Handbook for Electric Cooperatives* [Enervision, 2003], which has been issued by the Cooperative Research Network (CRN).

**The approach to securing MultiSpeak messages that is discussed in this document relies on good management of other aspects of cyber-security, such as effective password management and a good system of authorization that controls computer user access rights. MultiSpeak security will be effective only when applied as part of a more comprehensive approach.**

## 1.6 On-Going Security Developments

It is important to understand that the security concerns that are discussed in this document are not restricted to MultiSpeak communications. Indeed, they are not restricted just to the IT environment in the electric utility industry. These same cyber security issues are becoming critical in all industries.

You should be aware that there is a tremendous effort through the IT community, regardless of what industry it serves, to improve the security of data-intensive applications. The state-of-the-art in secure computing is changing rapidly. There are at least forty different security standards being considered for adoption in the

web services arena alone. Few of these are ready for implementation today, and none of them are as widely adopted as the solutions contained in this document. However, it is probable that better solutions for securing real-time computing systems will be available in the next few years. It is important that utility staff members responsible for developing security policies stay involved with what is happening in these areas and constantly re-evaluate whether the best solutions are being implemented.

Having stated this *caveat*, it is also important to understand that the solution discussed in this document is relatively simple, robust, and easy to deploy today. Properly implemented as part of a comprehensive IT security framework, it can provide enhanced security for the computing needs of most utilities.

## 2 Specific Risks and Countermeasures

- 2.1 Data System Security Services
- 2.2 Threats to MultiSpeak Data Messages
- 2.3 Approach to Provide Secure MultiSpeak Communications
- 2.4 Optimizing the Performance of Secured Applications

### 2.1 Data System Security Services

Before investigating the needs for securing MultiSpeak data exchanges, it is important to characterize the services expected of a secure computer system. A common classification of such services is given by Stallings [Stallings, 1995]:

- **Confidentiality.** This system service ensures that information stored or transmitted by a system is made available only to those users who are authorized to access the information.
- **Authentication.** This service provides identification of the originator of a message and proof that the originator is who he claims to be.
- **Integrity.** This function ensures that the messages transmitted using the system cannot be created, changed, deleted, or replayed except by authorized individuals and that the message received is identical to the one sent by the originating party.
- **Non-repudiation.** This characteristic of a message implies that neither the sender nor the recipient of a message can deny that the communication occurred.
- **Access Control.** This function restricts the use of the system data or resources to authorized parties.

### 2.2 Threats to MultiSpeak Data Messages

The threats to MultiSpeak-compliant messages include the following:

- **Interception.** Interception occurs when a communication is overheard by any party other than those authorized to receive it. *Interception is an attack on confidentiality.*
- **Fabrication.** Fabrication is the intentional insertion of false messages or data. It can take two forms (i) *masquerade*, when a new message with false content is inserted into the communications stream by an

unauthorized third-party, and (ii) *replay*, when a valid message is recorded and re-sent inappropriately by an unauthorized party. Utility operating systems are particularly sensitive to replay attacks. *Fabrication is an attack on authentication.*

- **Modification.** Modification occurs when a message is intercepted, the content is changed, and the communication is continued as if it had come from the original sender. *Modification is an attack on integrity.*

**Non-repudiation** typically is important only to systems that must ensure that actions occur exactly once and cannot be denied by either party later, such as banking or e-commerce applications. Although this security service is important in some situations, it is not considered important for the applications for which MultiSpeak data exchanges have been designed. Hence, no provisions for ensuring non-repudiation have been designed into the MultiSpeak security implementation.

**Access control** is a critical aspect of a comprehensive computer security plan. Controlling access, whether physical or electronic in nature, to the utility's computer and communications systems is important to ensure that the other security services can be maintained properly. Electronic access control consists, in part, of *authentication* which identifies a user and *authorization* which establishes the rights of that user to access or modify IT resources. An analogy can be made with a driver's license. It identifies the driver (authentication) and outlines the limits of what type of vehicle(s) the driver can operate (authorization).

All MultiSpeak messages *may* include a username and password pair, which can be used to identify and *authenticate* the message. However, in the base MultiSpeak specification, the use of a username and password to authenticate the message is optional. It is assumed that a strong means of restricting access to data and applications is in place where necessary. Hence, *authorization* is not covered in MultiSpeak. With the exception of message authentication, the larger issue of access control - although critical to the proper application of the security implementations suggested in this document - is outside the scope of this guideline.

While, it is assumed in this document that access to the utility's computers is secured, it is also assumed that MultiSpeak messages (both valid and attacks) may originate outside of the trusted network. As a result, the communications network is assumed to be untrustworthy; any desired security must be implemented at the message level.

The NERC *Security Guidelines for the Electricity Sector* [NERC, 2002] suggests that utilities implement user authentication for any access that permits "... *any command or control of a system, application or database, or allows any add,*

*modify, delete, or transmittal of any data...*” Thus user authentication is required as a minimum for any MultiSpeak communication that should be secured.

However, authentication alone merely ensures that the message being sent contains a means (such as username and password) that identifies a user recognized by the system. Without the addition of encryption, even properly authenticated messages are sent as clear, human-readable text. Thus, such messages would still be open to (i) interception, (ii) fabrication, and (iii) modification. Furthermore, an unencrypted message containing authentication provides sufficient information to a malicious interceptor to fabricate other messages that also include the same acceptable username and password. Thus a complete MultiSpeak messaging solution requires the implementation of both two-party authentication and message encryption.

To summarize, the solution proposed to secure MultiSpeak messages must provide confidentiality, authentication, and integrity. No single security function can provide all three services; however, the combination of message encryption and two-party authentication provides all of the required security services.

## 2.3 Approach to Provide Secure MultiSpeak Communications

The approach currently recommended for providing MultiSpeak message security is Secure Sockets Layer (SSL). SSL is undoubtedly the most widely adopted means to provide authentication and encryption to text messages sent over TCP/IP networks. If you have ever used a credit card on a secure web site, you have used SSL. Toolsets are available for supporting SSL on practically every commercial web server and software development platform in common use.

SSL relies on encryption to provide confidential data transmission and either one- or two-party user authentication to provide the authentication security service. The combination of encryption and user authentication ensures message integrity. SSL does not make any assumption about the security of the communication channel; hence, it is appropriate for use on an untrustworthy network. SSL merely assumes that the channel reliably transmits the data unchanged. Reliable transport is ensured in any TCP/IP network by the TCP (transport) layer. Thus nearly any protocol (such as HTTP, FTP, etc.) that can be sent over a TCP/IP network can support SSL. This flexibility enables MultiSpeak messages using any of the supported message transport mechanisms (batch, SOAP, TCP/IP sockets, web services) to be secured with SSL.

SSL is limited to point-to-point (two-party) messages. This is not a limitation to its applicability to MultiSpeak, since all MultiSpeak messaging is cast as point-to-point messages. Even point-to-multipoint (publish/subscribe) messages are considered to be multiple point-to-point messages in MultiSpeak. The only

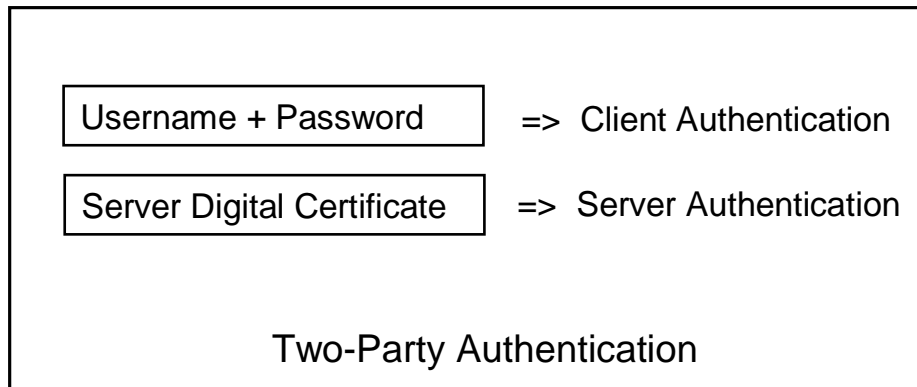
possible limitation to SSL that could affect its implementation in utilities is the fact that SSL is restricted to encrypting a message over a single point-to-point network link. If multi-hop network paths are necessary, each receiver must decrypt and re-encrypt the message, increasing the computational overhead. This will rarely be a concern for the types of messages envisioned, and even when multi-hop communications is necessary, it merely results in less efficient communications, not a loss in security.

Since SSL was originally designed to handle credit card transactions over the Internet, it was assumed that a credit card holder would want to authenticate the server to ensure that his credit card was not transmitted improperly to any third party. However, the credit card number itself was considered adequate authentication for the client. Thus SSL inherently handles server authentication, but client authentication is optional.

Server authentication in SSL is handled using digital certificates. It was assumed in the design of SSL that the overhead of maintaining a valid digital certificate for a commerce server was acceptable, but that customers might not purchase online if they had to obtain digital certificates to do so. Hence, client authentication, where it is implemented in SSL, relies on the client's public encryption key as an authentication string or on a username/password combination.

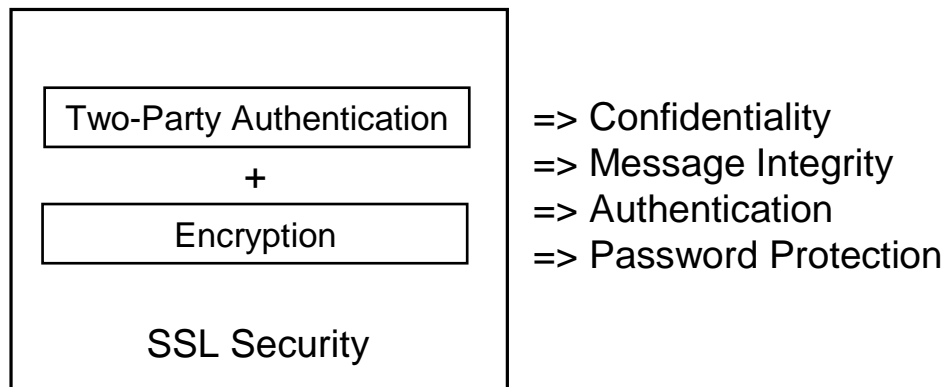
MultiSpeak messages all have the potential to pass optional usernames and passwords as a means to implement user authentication. Hence, for MultiSpeak messages, client authentication will be performed using the username/password pair carried by the MultiSpeak message header rather than using SSL client authentication with a public key. *It should be noted, that in the context of any on-going communication between two software applications in a utility, each software application may act alternately as client and server. Hence, nearly all software applications that must be secured must be capable of handling both username/password and certificate-based authentication.*

Figure 2-1 illustrates how two-party authentication is implemented in MultiSpeak messages.



**Figure 2-1 Two-Party Authentication In MultiSpeak**

Figure 2-2 shows that the combination of two-party authentication and message encryption provides all of the necessary security services outlined above.



**Figure 2-2 Components of SSL Security**

## 2.4 Optimizing the Performance of Secured Applications

It should be noted that communications may be significantly slower when SSL is implemented. According to Rescorla [Rescorla, 2001, pg. 175], SSL connections can be between 2 and 100 times slower than ordinary TCP connections. It should be noted that the choice of encryption key strength and the encryption algorithms chosen to implement SSL can significantly affect processing and communications speeds. Unfortunately, the same choices that reduce processing and communications overheads also reduce the protection afforded by using encryption. It is important to balance the need for strong encryption with the need for efficient communications.

Whether the overhead of SSL is justified in order to secure specific information exchanges or application interfaces is considered to be an issue to be addressed by utilities and their vendors, and is outside the scope of this document.

Similarly, the choice of key strength and the encryption algorithm used is considered outside the scope of this document, since it may be affected by (i) the SSL toolset or programming language used by your vendors, (ii) the limits of acceptable processing or communications overhead for any specific application, or (iii) the security needs of any specific data exchange. Utilities considering implementing MultiSpeak security should discuss these issues with their software vendors prior to purchasing or installing software.

## 3 Recommendations

### UTILITIES SHOULD TAKE THE FOLLOWING ACTIONS:

- **Use two-way authentication and encryption as described in this document if MultiSpeak interfaces are to be secured.**
- **Complete a comprehensive IT security plan.** The following subjects that affect secured MultiSpeak interfaces should be included:
  - Consider how to secure data exchanged among integrated systems, such as those linked with MultiSpeak.
  - Carefully consider the balance between system performance and the desired degree of security in designing countermeasures
  - Consider the special risks associated with real-time control systems, such as SCADA.
  - Address both internal and external security threats.
- **Implement a security policy.** It is important to remember that any security countermeasure that relies on authentication, such as the approach described herein for MultiSpeak interfaces, requires:
  - Adequate authorization and access control schemes.
  - Good password management.
  - Good control of physical access to sensitive systems.
- **Stay abreast of developments in IT security.**
- **Periodically re-evaluate your IT plan and the set of countermeasures adopted to ensure that the best available solutions are being used.**

### UTILITIES SHOULD DISCUSS THESE ISSUES WITH THEIR VENDORS:

- **Discuss whether the application of security is warranted in any MultiSpeak application, and its extent.**
- **Discuss potential risks to real-time control systems with software vendors. Address potential security countermeasures in these discussions, and consider the tradeoffs between improving security and impacting system performance.**
- **Discuss whether encryption is desired and if so the choice of encryption key strength.**

## 4 Glossary

**HTTP: *Hypertext Transfer Protocol.*** A protocol for exchanging text or hypertext data over TCP/IP networks. The implementation of SOAP and web services defined in this document uses HTTP carried over TCP/IP.

**Publish/subscribe:** A messaging paradigm where a client expresses interest in certain types of information by subscribing with a server component. The server component then asynchronously publishes information to clients that have previously subscribed.

**Real-time:** For this document, real-time is considered to be the asynchronous delivery of information as triggered by events, where message delivery is accomplished with no intentional time delay.

**Request/response:** a messaging paradigm where a client process requests information from a server process, which returns that information in the form of a response.

**SOAP: *Simple Object Access Protocol.*** SOAP is a standard that that facilitates the transport of XML formatted data, conceptually using any underlying transport. In the context of this document, SOAP transport uses HTTP over TCP/IP as a transport.

**SSL: *Secure Sockets Layer.*** A protocol used to secure TCP/IP network traffic using encryption and optional authentication services. SSL is a draft standard of the Internet Engineering Task Force, which is designed to provide security services to programs transferring data using TCP/IP protocols.

**TCP/IP: *Transmission Control Protocol/Internet Protocol.*** The transport and internet layer protocols used in the Internet and many intranets. Any of the real-time implementations of MultiSpeak messages (whether using SOAP, TCP/IP sockets, or web services) are assumed to use TCP/IP. File-based (batch file) transfers may use TCP/IP, other network protocols, or no network transport at all. This document applies to those circumstances where TCP/IP network protocols are used.

**Web service:** Any software service that is available over an intranet or the Internet, using a standardized XML messaging system and standard web protocols, and which is intended to be independent of operating system and programming language.

**XML: *Extensible markup language***, a flexible standard for information exchange. XML has the advantage of flexibly permitting the transfer of data in an extensible, structured manner. All MultiSpeak messages and data payloads are structured in XML-encoded text.

## 5 References

**[DHS, 2003]** Department of Homeland Security, *The National Strategy to Secure Cyberspace*, Washington D.C., 2003.

**[Enervision, 2003]** Enervision, Inc., *Information Technology Security Handbook for Electric Cooperatives*, First Edition, Arlington, Virginia, National Rural Electric Cooperative Association, 2003.

**[MultiSpeak, 2003a]** MultiSpeak Initiative, *MultiSpeak Version 2.2 Specification*, Arlington, Virginia, National Rural Electric Cooperative Association, 2003.

**[MultiSpeak, 2003b]** MultiSpeak Initiative, *MultiSpeak® Version 2 File-Based Transfer Implementation Guidelines*, Arlington, Virginia, National Rural Electric Cooperative Association, 2003.

**[MultiSpeak, 2003c]** MultiSpeak Initiative, *MultiSpeak® Version 2 SOAP Implementation Guidelines*, Arlington, Virginia, National Rural Electric Cooperative Association, 2003.

**[MultiSpeak, 2003d]** MultiSpeak Initiative, *MultiSpeak® Version 2 TCP/IP Sockets Implementation Guidelines*, Arlington, Virginia, National Rural Electric Cooperative Association, 2003.

**[MultiSpeak, 2004a]** MultiSpeak Initiative, *MultiSpeak® Version 2 Web Services Implementation Guidelines*, Arlington, Virginia, National Rural Electric Cooperative Association, 2004.

**[MultiSpeak, 2004b]** MultiSpeak Initiative, *MultiSpeak® Version 2 Security Implementation Guidelines*, Arlington, Virginia, National Rural Electric Cooperative Association, 2004.

**[NERC, 2002]** North American Electric Reliability Council, *Security Guidelines for the Electricity Sector*, Version 1.0, June 14, 2002.

**[Rescorla, 2001]** Rescorla, Eric, *SSL and TLS: Designing and Building Secure Systems*, First Edition, Boston, Massachusetts, Addison-Wesley, 2001.

**[Stallings, 1995]** Stallings, William, *Network and Internetwork Security: Principles and Practices*, First Edition, Englewood Cliffs, New Jersey, Prentice-Hall, Inc., 1995.