ASSESSMENT REPORT OF THE GAS INDUSTRY STANDARDS BOARD (GISB) ELECTRONIC DELIVERY MECHANISM RELATED STANDARDS

March 27, 2000

Prepared by
Sandia National Laboratories
Information Design Assurance Red Team
for the Department of Energy

Abstract

This document presents the results of an independent assessment of the standards developed by the Gas Industry Standards Board (GISB) related to its electronic delivery mechanisms. The assessment was conducted by Sandia National Laboratories' Information Design Assurance Red Team. The team was tasked not only with performing a thorough assessment and drawing relevant conclusions, but also with suggesting improvements that could be made, and using surety engineering to take into account the risk versus cost tradeoffs of the system being assessed. This document summarizes the assessment results and technical exchange analysis activities of the GISB Standards and provides evaluations based on these results.

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

Acknowledgments

This document was prepared for the Department of Energy (DOE) by a Working Group of the Information Design Assurance Red Team (IDART) at Sandia National Laboratories. The Working Group has the following members:

David Duggan, Technical Project Leader
Sandia National Laboratories
Secure Communication Systems
(505) 845-8100
dduggan@sandia.gov

Patricia Tempel, Technical Analyst
Sandia National Laboratories
High Integrity Software Systems Engineering Department
(505) 845-9889

phtempe@sandia.gov

Phillip Lewis, Technical Analyst
Sandia National Laboratories
Mission Engineering & Analysis
(505) 844-5308
pjlewis@sandia.gov

Tom Cabe, Project Leader
Sandia National Laboratories
Cryptography & Information Systems Surety
(505) 845-8032
tjcabe@sandia.gov

The working group would like to thank the following individuals from the Gas Industry Standards Board (GISB) for their contributions to this document:

Rae McQuade
Gas Industry Standards Board
Executive Director
(713) 356-0060
Carl Caldwell
CGI
Director Consulting Services
(713) 868-5537
Dick Brooks
Group 8760
Chief Technology Officer
(205) 250-8053
Jim Buccigross
Group 8760
Vice President, Energy Industry Practice
(508) 238-0345

Contents

EXECUTIVE SUMMARY **1**
1. Introduction **2**
2. Gas Industry Standards Board Description **2**
3. Objective and Purpose of the GISB Standards **2**
4. Critical Success Factors **2**
5. Metrics of Importance **3**
6. Surety Assessment Research **3**
7. Surety Assessment Analysis and Recommendations **4**
7.1 Security Issues **4**
7.1.1 Trading Partner Agreement (TPA) 4
7.1.2 Time Synchronization 4
7.1.3 Management of keys 4
7.1.4 Central Address Repository (CAR) 5
7.1.5 Encryption for Batch Processing 5
7.1.6 Interactive Processing 5
7.1.7 Secure Socket Layer (SSL) 6
7.1.8 Basic Authentication 6
7.1.9 Security Standards 6
7.1.10 Using a Web Server 6
7.1.11 Web Access Ports 7
7.1.12 Message replay attacks 7
7.2 Recommendations for GISB Principles **7**
7.2.1 Grouping of Principles 7
7.2.2 Future Technology Model 7
7.2.3 Principle 4.1.2 8
7.2.4 Principle 4.1.6 8
7.2.5 Principle 4.1.8 8
7.2.6 Principle 4.1.15 8
7.2.7 Principle 4.1.16, Principle 4.1.17 and Principle 4.1.19 9
7.3 Recommendations for GISB Standards **9**
7.3.1 Grouping of Standards 9
7.3.2 Standard 4.3.4 9
7.3.3 Standard 4.3.6 9
7.3.4 Standard 4.3.8 10
7.3.5 Standard 4.3.11 10
7.3.6 Standard 4.3.15 10
7.3.7 Consolidating like Standards 11
7.3.8 Standard 4.3.70 11
7.4 Other Areas for Improvement **11**
7.4.1 Document Tabs 11
7.4.2 Definitions and Acronyms 11
7.4.3 Web Pages 12
7.4.4 Reference Guide Section 12
7.4.5 GISB EDM document compatibility 12
7.4.6 Consistency of Terms 12
7.4.7 Clarify Encryption 13
7.4.8 Compliance Statement 13
8. Summary **13**
9. Conclusion **14**

Appendix A – References **15**
Appendix B – Abbreviations and Acronyms **16**

EXECUTIVE SUMMARY

This document provides an independent analysis of the standards developed by the Gas Industry Standards Board (GISB) related to its Electronic Delivery Mechanisms (EDM) described in a document titled "GISB Electronic Delivery Mechanisms Related Standards" and related documents. The Sandia Information Design Assurance Red Team (IDART) conducted the analysis and assessment of the GISB process.

This assessment was prepared by the Sandia Information Design Assurance Red Team at the request of the Department of Energy. The intent is to provide a surety based analysis of the current and any documented future GISB standards as they relate to electronic commerce. The assessment provides recommendations on the security of the electronic commerce guidelines for conducting business with emphasis on the use of the Internet.

The cooperation and assistance given to Sandia National Laboratories by GISB during this part of the assessment was timely and greatly appreciated.

The analysis focused primarily on the security of the EDM protocol as defined in the standards document, Version 1.4. Potential weaknesses have been identified. Communication concerning questions of interpretation ensued between GISB and Sandia. The following strengths of the GISB standards are recognized:

- Idea of principles, standards and definitions sections is good for creating a viable framework for electronic data interchange.
- Including the Future Technology Model early in the document provides an overview of the process for Trading Partners.
- Well designed layout of the document with good use of common look and feel techniques.

The following weaknesses in the security of the EDM were identified:

- Not all data in the transaction is encrypted.
- Not all transaction types are authenticated.
- There is no support to deny message replay attacks.
- Certain information, such as that contained in the Trading Partner's Agreement (TPA) and the Central Address Repository (CAR), are sources for an attacker.

The standards have changed from version 1.3 to version 1.4 during the course of this analysis. Improvements have been made in both the security area and the documentation area. Still, potential attackers on the Internet have improved their skills and tools and have shown their willingness to use both to cause problems for an industry. Keeping ahead of them will be important to GISB, as it relies more on the Internet as a transport mechanism for the EDM.

The Assessment Team believes that the GISB EDM Standards provide a valid base mechanism for the use of electronic commerce. The mechanisms provided by the standards, when used in accordance with the standards, afford reasonable protection to the partners. However, we believe there is opportunity for an adversary to affect the system in a negative way, even to the point of forging transactions. With the addition of some incremental security measures, these standards can become more resistant to malicious activity than they currently are today.

The Internet can provide industry with better communication than ever before, but also has additional opportunity for problems when security is not the foremost premise for this communication. Potential attackers on the Internet will continue to improve their skills and tools. Keeping ahead of them will be important to GISB, as it moves to operate over the Internet.

1. Introduction

This document provides an independent analysis of the standards developed by the Gas Industry Standards Board (GISB) related to its Electronic Delivery Mechanisms (EDM) described in a document titled "GISB Electronic Delivery Mechanisms Related Standards". The Sandia Information Design Assurance Red Team (IDART) conducted the analysis and assessment of the GISB process.

The Sandia team operated on the principle that an independent analysis should include a comprehensive assessment and suggested improvements while incorporating surety engineering concepts throughout the study. Surety can be defined as a measure of the assurance of system reliability, safety, security and control of use, while balancing denial of unauthorized use with assurance of authorized use within the constraints of risk versus cost.

This assessment was prepared by the Sandia Information Design Assurance Red Team at the request of the Department of Energy. The intent is to provide a surety based analysis of the current and any documented future GISB standards as they relate to electronic commerce. This assessment provides recommendations on the security of the electronic commerce guidelines for conducting business with emphasis on the use of the Internet.

2. Gas Industry Standards Board Description

The Gas Industry Standards Board (GISB) is a nonprofit North American industry association whose mission is "to develop and promote standards to simplify and expand electronic communications, and to simplify and streamline business practices that will lead to a seamless marketplace for natural gas". These standards are to assist the natural gas industry in improving customer service, enhancing the reliability of natural gas service and increasing the competitiveness and efficiency of natural gas markets.

3. Objective and Purpose of the GISB Standards

The evolution of the Internet into the principal medium for electronic communications in worldwide commerce led GISB to develop standards for the use of the Internet by the gas industry to transact business. Gas transmission companies are establishing Internet sites, including server sites for electronic interchange of files and world wide web pages, to provide information to shippers and other customers. These sites supplement, and will eventually replace, pipelines' electronic bulletin boards (EBBs). These sites allow Local Distribution Companies (LDCs) and other service requesters to place orders and receive scheduled quantity reports (statements indicating that the gas has been scheduled by the pipeline) electronically.

The standards also allow for third party providers (represented by GISB's service sector) to provide buyers of natural gas, transportation and other services with a "one-stop shopping" capability that will avoid the necessity of communicating with multiple Internet sites in order to complete a transaction. One way the standards accommodate this service is by providing a 15-minute window after the nomination deadline to communicate information. All GISB transactions on the Internet are encrypted to protect their privacy and integrity.

4. Critical Success Factors

Several critical success factors have been identified during analysis of the GISB Electronic Delivery Mechanism Related Standards. These factors will help determine if the GISB Standards increase security of electronic delivery for the Gas Industry. Critical Success Factors identified include the following:

- Gas Industry Trading Partners must adopt GISB Standards for the use of electronic delivery of critical information.
- Internet Delivery Mechanism moves data across the internet in a secure manner following the prescribed GISB future technology model.
- Web sites including Customer Activities and Informational Posting must follow GISB standards for content and security.
- Trading Partner Agreement must be properly completed by involved parties and the paper copy protected to avoid details being disclosed to unauthorized parties.
- Data must be transmitted in the accepted standard data format.
- The authenticity of all Internet transactions must be verifiable.

5. Metrics of Importance

Metrics should be collected and analyzed to measure how the implementation of GISB EDM Standards increases the security and reliability of electronic data exchanges between trading partners. The following are some examples of metrics that could be collected for GISB Standards (possibly by incorporating the statistic collectors within the standards framework):

- Measure how many companies are implementing GISB Standards (update monthly)
- Measure the volume of transactions sent via EDM each month. (Keep categories separate, e.g. Batch, interactive, interactive flat file, etc…)
- Measure the dollar amount of EDM transactions each month or cubic feet of gas
- Capture the number of Computer Security Incidents at GISB sites each month (self reported)
- Measure average response time of EDM transactions each month (how many exceed 15 minutes)
- Measure the level of compliance for each trading partner pair. (Level of security compliance, e.g. No encryption, 40-bit SSL, 128-bit SSL).

Most of these can be self reported on a statistics page maintained by each partner. That page should allow only authenticated access. If possible, GISB could collect and tabulate the totals annually.

6. Surety Assessment Research

Research of the GISB Standards by Sandia's IDART Team began with an analysis of version 1.3 of the EDM Standards. Version 1.3 was dated July 31, 1998 and provided the best information available when the analysis began. Version 1.4 has since been issued (November 15, 1999) with updated and improved standards. The Sandia Team shifted its focus to version 1.4 and the analysis and recommendations are based on information in this most recent version.

Generally the issues noted in this section (6) relate to higher levels of implementation, security, and information management as they were revealed during analysis of the GISB Standards. These issues do not specify levels of criticality or likelihood, nor are they intended to suggest priority of resource allocation.

1. The Sandia Team feels that the idea of principles, standards and definitions as outlined in version 1.4 provides a viable framework for electronic data interchange. Including the Future Technology Model early in the document provides a good overview of the process for Trading Partners. Version 1.4 appears to have a well designed layout and makes good use of common look and feel techniques.

2. Several security issues and concerns were identified in the initial analysis of version 1.3. Some of these were addressed in version 1.4. However, several security concerns about the GISB Standards remain and are addressed in this document.
3. GISB Standards allow for the use of unsecured transactions between partners not wishing to be secure. This opens the possibility of third parties gathering information from these transactions and using this information later to plan an attack. Other identified security issues are discussed in detail in section 7.
4. The Sandia Team feels that there are improvements which can be made to the actual GISB Standards document itself. Specifically the Future Technology Model needs clarification and refinement. Sandia also recommends some changes to the version 1.4 document. These changes are covered in detail in sections 7.2, 7.3, and 7.4 of this report.

7. Surety Assessment Analysis and Recommendations

The analysis focused on the Gas Industry Standards Board Electronic Delivery Mechanism Related Standards. The Sandia Assessment Team recommends that GISB consider the following analysis and recommendations to improve the Electronic Delivery Mechanism Related Standards.

7.1 Security Issues

Items listed in the following section deal specifically with areas of opportunity for an attacker within the guidelines set forth by the security standards. The order provided in this section does not imply importance.

7.1.1 Trading Partner Agreement (TPA)

The expectations of who will perform what function and how it will be accomplished in Internet EDM is, at some level, laid out in the Trading Partner Agreement.

Analysis: The TPA is an important document necessary to establish the trading partnership between companies. This document contains information, including usernames and passwords, needed to access each partner's network and should be protected from unauthorized exposure.

Recommendation: Each trading partner should protect the TPA as a proprietary company document.

7.1.2 Time Synchronization

The time-stamp should be included in the HTTP response back to the sender of the original HTTP transaction. It is recommended that the server clock generating the time-stamp be synchronized with the National Institute of Standards and Technology (NIST) time in order to mitigate discrepancies between the clocks of the sender and receiver. (Standard 4.3.10)

Analysis: There is a need for client machines to verify that the time on the server is within a certain "delta" time. By modifying the time on a server, it is possible to "game" the system by either shutting off transactions early, or by giving an insider extra time to examine other's transactions. By having the client check time on the server, it can notify the user of a possible problem with the time on the server.

Recommendation: Define a standard that requires clients to acquire time-of-day from the server and check that time against their own time reference. If the time difference is greater than say, ten seconds notify the user of the discrepancy.

7.1.3 Management of keys

How to manage keys is covered in the TPA (exchange, verifying, changing, making keys and replacing keys).

Analysis: We realize that there is overhead involved in the exchange of new keys, but the risk of having a key become compromised is greater the longer the key is in use. Operationally, keys could be set to expire 385 days (365 days plus a cushion) after being created to allow for yearly re-keying on a regularly scheduled basis.

Recommendation: It is recommended that keys expire at least on a yearly basis. By expiring keys yearly, the mechanisms for exchanging keys are exercised on a regular basis and keys do not have an infinite lifetime, thereby reducing the likelihood of a key compromise.

7.1.4 Central Address Repository (CAR)

Standard 4.3.19 states that the CAR should make available a consolidated repository of the Transportation Service Providers' current URLs listed in Standard 4.3.18 in two ways: 1) a vehicle to link to sites and categories, and 2) a downloadable list.

The CAR is available to any Internet user.

Standard 4.3.20 states that a userID or password should not be required to access the Central Address Repository or the Transportation Service Provider's Informational Postings web site.

Analysis: The CAR can be used as an attack list for a malicious individual. Leaving the CAR unprotected and available to any Internet user can result in attacks being directed at the customers of a specific site. It is tailor made for attacking using a denial-of-service type of attack.

Recommendation: Protect the CAR using SSL and basic authentication. It is recommended that the standard be reworded to state that a userID and password be required to access the CAR for security purposes. The access password can be a single userID/password combination created, and changed yearly, by GISB for the member organizations, but implemented locally by each member. The userID/password can be distributed securely by the GISB office to members.

7.1.5 Encryption for Batch Processing

PGP 2.6 (using keys generated with the RSA algorithm) is used for encryption and digital signatures on batch data. The header information in the POST operation is not encrypted.

Analysis: Header information from batch processing can be used to forge packets for use in the interactive type of process. There is also a wealth of information to be gained by an attacker from the responses that are useful in defining attack strategies.

Recommendation: Batch processing of requests should be encrypted using SSL. Response messages to requests should be encrypted also.

7.1.6 Interactive Processing

Interactive processing does not require strong authentication of the user before processing a transaction.

Analysis: Interactive processing can be spoofed since there is no PGP signature present for the transaction. Without strong authentication of the transaction, the sender can be anyone. By acquiring response messages from some client-server communication, an attacker has enough information to create a transaction spoofed as someone else.

Recommendation: Add a standard that requires PGP signatures for interactive processing of transactions under SSL encryption protection. Define responses that are available under the interactive processing. PGP allows for digital signing and encryption of data contained on the clipboard. This method can be used to sign interactive data.

7.1.7 Secure Socket Layer (SSL)

40 bit SSL is the basic standard, while 128 bit SSL is preferred.

Analysis: 40 bit SSL offers some protection. It has been around for a long time (in computer time) and is nearing the end of its useful lifetime. Performance of computers is such that 40 bit SSL will be able to be broken in minutes in the near future. 40 bit SSL was broken in 1996 by a student in less than 8 hours of computer processing time. Since GISB only changes standards infrequently and all changes must be approved by the members, it should start acting now to require 128 bit SSL instead of 40 bit.

Recommendation: 40 bit SSL should be changed to 128 bit SSL on standards 4.3.61 and 4.3.83. All basic client authentication should be done under the protection of 128 bit SSL.

7.1.8 Basic Authentication

Basic Authentication is in standard 4.3.84 and is outlined in the "Sending Transactions" section and in the "Security" section under Security Requirements. HTTP basic authentication includes a userID and password. Basic authentication is also known as realm one security.

Analysis: GISB standards allow for the use of unsecured transactions between partners not wishing to be secure. Should these transactions be compromised, there will be damage to the credibility of the GISB standards as a secure EDM.

Recommendation: In the "Security" section under Basic Authentication remove the statement “Those companies who wish to conduct business across the Internet in an unsecure fashion may do so by mutual agreement.”

7.1.9 Security Standards

Currently GISB has a set of minimum security standards, which can be found in the GISB standards and in the TPA. The basic security standards include: functional acknowledgements, basic authentication, PGP, and key management.

Analysis*:* Utilization of these standards completely and consistently is important. Use of PGP encryption and/or signatures on all transactions, whether batch or interactive, will help the security of the system. As long as the Gas industry is not considered an active target by an individual, or a group, lax use of the standards can be allowed to occur. However, a single individual working alone, with reasonable knowledge of the GISB standards can work to undermine the electronic commerce of the industry.

Recommendation*:* Require the use of strong encryption and strong authentication on all transactions.

7.1.10 Using a Web Server

In Tab 6 section "Receiving Transactions", GISB does not currently require either a Secure Sockets Layer (SSL) or Secure Hyper Text Transfer Protocol (S-HTTP). This forces the sending of userIDs and passwords in the CLEAR. GISB does recommend SSL for flat file EDM in standard 4.3.83.

Analysis: Establishing an SSL session prior to the HTTP POST process (whether it is batch or interactive) protects the userID, password and any header information. This information can be used to create spoofed transactions by an attacker.

Recommendation: Require the use of strong encryption and strong authentication on all transactions.

7.1.11 Web Access Ports

GISB is using non standard ports (5713, 6112, 6304, 6874, and 7403) for access to web servers. GISB limits the TCP ports used as a standard for EDM communications standards 4.1.37 and 4.3.70. GISB states that non-standard ports in a non-privileged range adds another level of security.

Analysis: Port numbers can be scanned in a matter of minutes, therefore using non-standard ports doesn't afford any protection. Using ports that are allocated to another service can give opportunity for conflict at a user site. Additional ports in the list should be taken from an unallocated portion of the port space.

Recommendation: Use standard TCP ports for web servers. If that option is not viable, use ports that are not already allocated to other services.

7.1.12 Message replay attacks

Message replay is not addressed in the standards.

Analysis: Currently there is no mechanism in place that will disallow replay attacks. Both client and server mechanisms need to be in place to keep this from being a viable attack.

Recommendation: By having the client check time on the server before sending any transactions, it is possible to include a time field in the header information. A server then should not be allowed to process two orders from the same requester using the same time stamp. This method will only work if the transaction is digitally signed using an accepted cryptographic checksum. An example of such an algorithm is the Secure Hash Algorithm defined in FIPS Pub 180-1. PGP uses an accepted cryptographic checksum algorithm.

7.2 Recommendations for GISB Principles

7.2.1 Grouping of Principles

The principles outlined in Tab 4 pages 8-11 appear in chronological order according to GISB correspondence.

Analysis: The principles are a key component of the standards document and are important guidelines for trading partners. The principles cover topics that can be grouped together in similar categories. Some principles lend themselves to consolidation.

Recommendation: Consider grouping similar principles into like categories such as:

- Common Governance Guidelines and Principles→ 4.1.x
- Web site or Web Page Principles → 4.2.x
- Data Formatting Principles → 4.3.x

Consider consolidating the number of principles when two or more principles appear similar. For example 4.1.17, 4.1.18 and 4.4.19 could be consolidated into one principle.

7.2.2 Future Technology Model

In version 1.4 of the EDM Standards the Future Technology Model diagram on page 8 Tab 4 appears unchanged from version 1.3. The model includes numbering 1 through 6 and depicts the electronic interchange of data.

Analysis: The model is an important diagram that outlines the EDM flow. There are two sentences that describe the technology and mechanisms in terms of the customer and provider.

Recommendation: Clarify the Future Technology Model to describe what each of the six numbers refer to. Also consider moving the model to its own page as is done with the Batch Flow Diagram later in the document. If the third party system participation is optional show it as such. Describe the sequence of events that the diagram is trying to illustrate. Also it can stand alone as a diagram and does not need to be numbered as a principle.

7.2.3 Principle 4.1.2

This recommendation references Principle 4.1.2 and provides suggested rewording of this principle.

Analysis: Principle 4.1.2 states: "The Electronic Delivery Mechanism does not pick winners, rather it should create an environment where the marketplace can dictate a winner or winners." This principle is not clear.

Recommendation: This principle is not clear and should be reworded. Consider rewording as follows: "The EDM process and related principles will evolve over time into a market directed set of standards to govern EDI."

7.2.4 Principle 4.1.6

This recommendation references Principle 4.1.6 and provides suggested rewording of this principle

Analysis: Principle 4.1.6 states: "Data providers (transportation service providers) should interface with third party vendors according to GISB standards." This principle is not clear.

Recommendation: Consider rewording as follows: "Data providers (transportation service providers) should interface with 3rd party vendors, when required, and follow GISB standards for EDM."

7.2.5 Principle 4.1.8

This recommendation references Principle 4.1.8 and provides suggested rewording of this principle.

Analysis: Principle 4.1.8 states: "The same business result should occur regardless of the electronic delivery mechanism: this principle should guide the definition of the business process, data content of the transaction, and the timing of the transaction." The Sandia Team feels that this is a key principle that is well written. This principle sets the foundation for many of the other principles.

Recommendation: As recommended earlier like principles should be grouped together. It is recommended that this principle be grouped within the governance principles. It is also recommended that it be moved to the first or second principle within this group.

7.2.6 Principle 4.1.15

This recommendation references Principle 4.1.15 and provides suggested rewording of this principle.

Analysis: Principle 4.1.15 states: "The GISB should not set standards for site-level security. Individual organization security standards should be relied upon." This principle seems to contradict standard 4.3.15. Standard 4.3.15 seems to recommend that a basic level of security features be implemented.

Recommendation: Consider revising principle 4.1.15 to include concepts stated in standard 4.3.15. Possible wording of Principle 4.1.15 is the following: "The GISB will recommend a minimum level of standards for site level security. Individual organization security standards should be integrated with the recommended GISB minimum standards."

7.2.7 Principle 4.1.16, Principle 4.1.17 and Principle 4.1.19.

This recommendation references Principle 4.1.16, Principle 4.1.17 and Principle 4.1.19 and provides suggested rewording of these principles.

Analysis: The statements "easy to locate" and "easy to download" can be interpreted in many ways. These statements leave the meanings open to individual interpretations of the trading partners and therefore individual implementations.

Recommendation: Consider consolidating these principles into one and consider rewording such as: "Informational Postings Web sites should be accessible by all members, and the information contained on these web sites should be downloadable."

7.3 Recommendations for GISB Standards

7.3.1 Grouping of Standards

The standards outlined in Tab 4 pages 12-24 appear in chronological order according to GISB correspondence.

Analysis: The standards are a key component of this document and provide valuable information to the member trading partners. These standards cover topics that can be grouped together into similar categories. Some standards may also lend themselves to consolidation.

Recommendation: Consider grouping similar standards into like categories rather than chronologically. Such grouping may include:

- Data Transmission Standards
- Data Formatting Standards
- Browser and Time stamping Standards
- Informational Posting Standards
- Customer Activities Web sites Standards

Also consider consolidating the number of standards when two or more appear very similar.

7.3.2 Standard 4.3.4

This recommendation references Standard 4.3.4 which states: "Transactional data should be retained for at least 24 months for audit purposes."

Analysis: This standard involves a critical distinction for member partners. The ability to track transactional data is certainly a desirable goal for any system.

Recommendation: This standard needs some clarification before it can be implemented, specifically, who should retain this data. Party A? Party B? Both? Also the volume of data generated should be a consideration. Will there be additional storage expense and/or security concerns raised with the implementation of this standard?

7.3.3 Standard 4.3.6

This recommendation involves Standard 4.3.6 which states: "Transportation Service Providers should make all pertinent EBB functions and information available via the Internet or via the technology recommended by GISB within a reasonable amount of time after each such function or information has become standardized as appropriate by GISB."

Analysis: While the intention of this standard is well received, the actual implementation of it as written is unclear. A standard that states "within a reasonable amount of time" is open to interpretation by members.

Recommendation: Make this standard more specific. State exactly what GISB thinks is a reasonable amount of time. The Sandia Team believes that one month is a reasonable amount of time to incorporate the new standard to their processes, given that members have been afforded the opportunity to participate in the definition of any standards changes. GISB should include a specific time frame into the wording of this standard.

7.3.4 Standard 4.3.8

This recommendation refers to Standard 4.3.8 which states: "The minimum acceptable protocol standard should be HTTP. All sending and receiving parties should be capable of sending and receiving using HTTP."

Analysis: This is an important standard for all EDM transactions. This standard should be clearly defined for all member trading partners.

Recommendation: Clearly state which version of HTTP should be used in this standard. On page 7 under Security it mentions the HTTP 1.0 specification. GISB should state which version of HTTP and HTTPS are to be used for EDM transactions. It is also important to update these standards at least yearly as technology changes dictate.

7.3.5 Standard 4.3.11

This recommendation refers to Standard 4.3.11 which states: "The HTTP response should be sent to the sending IP address. Other response documents should be returned to the official designated site defined in the TPA."

Analysis: This allows the initial message response to be sent to the IP address of the incoming message, whereas further traffic is sent to the IP address in the TPA, possibly a different address. This arrangement appears to offer an excellent opportunity to spoof the system. Reliance on IP addresses also allows an adversary to use IP spoofing to attack the system.

Recommendation: Sandia recommends a mechanism be put in place to "close the loop" between the possibly two different IP addresses to prevent this from being a problem. This could be done by either changing the standard to allow only one address to be used for all responses, or defining a mechanism to be used to reconcile responses sent to different addresses.

7.3.6 Standard 4.3.15

This recommendation refers to Standard 4.3.15 which states: "Trading partners should implement all security features using a file based approach via a commercially available implementation of PGP 2.6 or greater. Trading partners should also implement basic authentication. This should be regarded as an interim solution since this technology is not an open standard. This technology supports all of the above security features while providing independence of choice of Web servers and browsers. Encryption keys should be self-certified and the means of exchange should be specified in the Trading Partner Agreement."

Analysis: The Sandia Team feels this standard as written is too lengthy and combines many important standards.

Recommendation: This standard contains several important aspects of GISB security. It is recommended that this standard be clarified and broken down into three separate security standards. For example:

- Server Authentication
- SSL encryption

- PGP 2.6 or compatible

7.3.7 Consolidating like Standards

Standards 4.3.36, 4.3.37 and 4.3.38 all address similar internet concerns.

Analysis: These three standards all address similar internet concerns and provide an opportunity to combine like standards.

Recommendation: Consider combining these three standards into one standard with wording such as: "Industry web sites should be accessible via the public Internet using TCP/IP and Internet Compatible browser software."

7.3.8 Standard 4.3.70

This recommendation refers to Standard 4.3.70 which states: "Transportation Service Providers should be limited to the GISB approved list of available TCP ports and UDP ports of EDM implementation included in the Appendix of the EDM standards manual under Client Firewall Requirements for Service Provider EDM Implementation."

Analysis: This is actually included in Tab 4 under the TCP Communications section.

Recommendation: Change the reference from 'Appendix' to 'Tab 4 Business Process and Practices under TCP communications section'.

7.4 Other Areas for Improvement

The following recommendations are submitted for consideration in the format and layout of the standards document:

7.4.1 Document Tabs

The current EDM Related Standards document, Version 1.4, contains Tabs 1-10 and each tab starts with page 1.

Analysis: The renumbering of each tab in this important document could lead to confusion if readers are looking to quickly locate a specific page or section. The idea of 10 different page number 1's in the same document may confuse some readers. There also appears to be a Tab missing between Tab 6 and Tab 7.

Recommendation: Consider the notion of numbering the pages of each Tab sequentially, starting at 1, continuing to the end of the Tab. In the Table of Contents the Tabs will remain the same and the beginning page numbers can be added to the right. Example Tab 1 … Page 1-1

Tab 2 … Page 2-1

Tab 3 … Page 3-1

There appears to be an entire Tab section missing from the Table of Contents in version 1.4. In the document between Tab 6 and Tab 7 there is a 28 page section that appears to be a separate section. It begins with a Batch Flow Diagram. Either renumber this as a part of Tab 6 or Tab 7 or create a new Tab 7 and renumber the remaining Tabs.

7.4.2 Definitions and Acronyms

In the current version 1.4, Tab 4 contains the following sections in order starting with Principles on page 8 , Definitions on page 11, and Standards on page 12.

Analysis: The definitions section does not seem to belong in the middle of principles and standards sections. It affects the flow and readability of the document. Also it is noted that some key acronyms are used in the document before they are defined.

Recommendation: Consider moving the Definitions section to the front of Tab 4 before the principles and standards section. This will help the reader understand key terms and provide a quick reference point. Define key acronyms the first time they are used in the document. Define "Internet Compatible" and "Upstream/Downstream Identifier".

7.4.3 Web Pages

Tab 8 describes the Technical Implementation of the EBB/EDM functionality. This section covers important aspects of web sites including page layout, navigation, forms, matrix and lookups.

Analysis: The Sandia Team feels this is an important section and conveys many key concepts to members. The page layout section is well written and the print screen examples are very helpful.

Recommendation: GISB may consider taking this section one step further and developing a sample or model web site which includes these layouts and concepts. The web site could then be referenced as a URL within Tab 8 and allow the Trading Partners the ability to link to actual examples. This may help the partners actually view the examples and gain a better understanding of the formatting, layout, and common look and feel.

7.4.4 Reference Guide Section

In Tab 10 Appendix A the Reference Guide section defines reference information for some key concepts.

Analysis: This is an important reference section for Trading Partners and GISB members.

Recommendation: Consider adding two additional items and related references to this section. We recommend that the Guideline Adoption Procedure and X12.58 encryption standard entries be added. The Sandia Team also recommends that this section be reviewed and updated periodically as needed.

7.4.5 GISB EDM document compatibility

The GISB EDM version compatibility is not discussed in the standards document or the Trading Partner Agreement.

Analysis: It is noted that both parties need to support the same GISB EDM version. If the parties do not support the same version there should be an error message of notification to state there is a mismatch of the EDM version number.

Recommendation: It is recommended that both parties (trading partners) should support the same GISB EDM version. This should probably be stated in the Trading Partner Agreement. New standards should also include a statement about the compatibility with previous versions of the standard.

7.4.6 Consistency of Terms

In Tab 4 page 10 item 4.1.23 mentions the Standard Client Configuration and in Tab 9 page 7 the encryption section mentions the Client Configuration Standard.

Analysis: Important terms and concepts should be referred to in a consistent manner throughout the document.

Recommendation: Change Tab 9 page 7 wording to "Standard Client Configuration". Look for other key concepts in terms of consistent wording and usage.

7.4.7 Clarify Encryption

The document references encryption of batch data on page 19 between Tabs 6 and 7. This section also addresses decryption and signature verification.

Analysis: The document specifies very clearly when and how the transactions should be decrypted, but provides only general references to the fact that the transactions are encrypted.

Recommendation: Clarify where and how it is expected that the encryption take place in the process. Provide additional details on the encryption.

7.4.8 Compliance Statement

There is no definition statement of compliance to the GISB standards.

Analysis: In the standards document, there are several places where the member is given a choice between different levels of security. These options have some significance on security of the EDM. If these choices are still to be contained in the document, then there should be several levels of compliance defined for the standards. For example, compliance with all the standards and using 40 bit SSL encryption could be defined as being "Compliant to GISB version 1.4, weak encryption", while the same situation using 128 bit SSL instead could be defined as "Compliant to GISB version 1.4".

Recommendation: If there are security choices allowed in the standards, define specific titles for the compliance level to the standard.

8. Summary

The Sandia Assessment Team conducted an analysis of GISB EDM Standards. The cooperation and assistance given to Sandia National Laboratories by GISB during this part of the assessment was timely and greatly appreciated.

The analysis focused primarily on the security of the EDM protocol that is being defined in the standards document, Version 1.4. Potential weaknesses have been identified. Communication concerning questions of interpretation ensued between GISB and Sandia. The following strengths of GISB were recognized:

- Idea of principles, standards and definitions sections is good for creating a viable framework for electronic data interchange.
- Including the Future Technology Model early in the document provides an overview of the process for Trading Partners.
- Well designed layout of the document with good use of common look and feel techniques.

The following weaknesses in the security of the EDM were identified:

- Not all data in the transaction is encrypted.
- Not all transaction types are authenticated.
- There is no support to deny message replay attacks.
- Certain information, such as that contained in the TPA and the CAR, are sources for an attacker.

The standards have changed from version 1.3 to version 1.4. Improvements have been made in both the security area and the documentation area. Still, potential attackers on the Internet have improved their skills and tools and have shown their willingness to use both to cause problems for an industry. Keeping ahead of them will be important to GISB, as it relies more on the Internet as a transport mechanism for the EDM.

9. Conclusion

This report is intended to contribute to the improvement of GISB EDM Standards, and was developed with the best information available at the time.

The Assessment Team believes that the GISB EDM Standards provide a valid base mechanism for the use of electronic commerce. The mechanisms provided by the standards, when used in accordance with the standards, afford reasonable protection to the partners. However, we believe there is opportunity for an adversary to affect the system in a negative way, even to the point of forging transactions. With the addition of some incremental security measures, these standards can become more resistant to malicious activity than they currently are today.

The Internet can provide industry with better communication than ever before, but also has additional opportunity for problems when security is not the foremost premise for this communication. Potential attackers on the Internet have improved their skills and tools and have shown their willingness to use both to cause problems for an industry. Keeping ahead of them will be important to GISB, as it moves to operate over the Internet.

Appendix A – References

[1].Gas Industry Standards Board, *Electronic Delivery Mechanism Related Standards*, Version 1.4, November 15, 1999

[2].Gas Industry Standards Board, *A Concise Guide to GISB*, 1997.

[3].Gas Industry Standards Board, *Electronic Data Interchange Trading Partner Agreement*, Standard 6.3.3, 1998

[4] Gas Industry Standards Board, *Responses to Sandia National Laboratories Questions forwarded on February 25*, 2000, dated March 5, 2000

[5] Gas Industry Standards Board, *Business Practice Standards - Standards and Models Relating to Nominations, Flowing Gas, Invoicing, Electronic Delivery Mechanisms, Capacity Release, Contracts, and Interpretations*, Version 1.4, August 31, 1999

Appendix B – Abbreviations and Acronyms

CAR	Central Address Repository
DOE	Department of Energy
EBB	Electronic Bulletin Board
EDI	Electronic Delivery Interface
EDM	Electronic Delivery Mechanism
FTP	File Transfer Protocol
GAP	Guidelines Adoption Procedure
GISB	Gas Industry Standards Board
GUI	Graphical User Interface
HTTP	Hyper Text Transfer Protocol
IDART	Information Design Assurance Red Team
NIST	National Institute of Standards and Technology
PGP	Pretty Good Privacy
S-HTTP	Secure Hyper Text Transfer Protocol
SSL	Secure Socket Layer
TPA	Trading Partner Agreement