GAS INDUSTRY STANDARDS BOARD RESPONSE

TO THE

SANDIA NATIONAL LABORATORIES

SURETY ASSESSMENT REPORT OF THE

GISB ELECTRONIC DELIVERY MECHANISM RELATED STANDARDS

May 1, 2001

Prepared by

GISB Electronic Delivery Mechanisms Subcommittee
GISB Future Technology Subcommittee

Acknowledgments:

This document was prepared by the Electronic Delivery Mechanisms Subcommittee and the Future Technology Task Force of the Gas Industry Standards Board in response to the surety assessment prepared by the Sandia National Laboratories.

The chairs of the above subcommittee and contributors to this report are:

- Richard Brooks — Chief Technical Officer ,Group 8760
  Co-Chair, GISB EDM Subcommittee
- Richard Hamilton — Technical Consultant, Williams Gas Pipeline
  Contributor, GISB EDM Subcommittee
- Jim Keisler — Systems Analyst Consultant, Williams Gas Pipeline
  Contributor, GISB EDM Subcommittee
- Terry Lehn — Information Technology Consultant, Enron Transportation Services
  Contributor, GISB EDM Subcommittee
- Michael Shahan — Manager Information Technology Services, Dominion
  Chair, GISB Future Technology Task Force
- Leigh Spangler — President, Latitude Technologies
  Co-Chair, GISB EDM Subcommittee

Executive Summary:

GISB Responses to the Sandia Surety Assessment Findings:

7.1.1 Trading Partner Agreement (TPA)

Sandia Finding: 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.

Sandia 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.

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

GISB Response: We concur with the finding, analysis and recommendation. To implement the recommendation, the following note will be added to the face of the TPA: "Recognizing that this Trading Partner Agreement (TPA) is a confidential document whose revelation could jeopardize the commerce and communication that is conducted between the parties to this agreement, the parties should take at least the same amount of care to secure this TPA as would be taken with any other proprietary, internal or contractual document."

7.1.2 Time Synchronization

Sandia Finding: 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)

Sandia 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.

Sandia 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.

GISB Response: We concur with the finding, analysis and recommendation. To implement the recommendation, the GISB Standard 4.3.10 will be changed as follows:

4.3.10 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 should be synchronized with the National Institute of Standards and Technology (NIST) time in order to mitigate the discrepancies between the clocks of the sender and receiver.

With this change, the language is strengthened and the implementers of GISB standards have the opportunity to propose other mechanisms that would further enhance coordination of server clocks.

7.1.3 Management of keys

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

Sandia 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.

Sandia 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.

GISB Response: We concur with the finding and the analysis. To mitigate the risk, we will change GISB Standard No. 4.3.15 to require that keys should have a limited lifetime, the lifetime to be determined by the key's owner. Below is the language for the new standard:

4.3.15 Trading partners should implement all security features (secure authentication, integrity, privacy, and non-repudiation) using a file-based approach via a commercially available implementation of PGP 2.6 or greater (or compatible with PGP 2.6). 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. Encryption keys should have a limited lifetime whose duration is determined by the key's owner. A key's end of life is expressed in the expiration date field contained in each PGP public key. A lifetime of one year or less is recommended.

GISB Responses to the Sandia Surety Assessment Findings:

7.1.4 Central Address Repository (CAR)

Sandia Finding: 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.

Sandia 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.

Sandia 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.

GISB Response: We concur with the finding and the analysis. However, for the central address repository, the recommendation that GISB use both SSL encryption and a logon authentication would hinder the public from convenient and easy access, and possibly block access for legitimate users, while protecting against an unlikely risk. Several government agencies also make URL listings available for access and download without SSL encryption and logon authentication. Because of the unlikely event of an attack, the cost to implement such security measures, and the barriers to easy access by the public, GISB at this time will not implement the security measures of SSL encryption and logon authentication for the Central Address Repository.

7.1.5 Encryption for Batch Processing

Sandia Finding: 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.

Sandia 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 strategis.

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

GISB Response: We concur with the finding, analysis and recommendation. Batch processing of requests should be encrypted using SSL with 128-bit encryption and Response messages to requests should be encrypted also using SSL with 128-bit encryption. Programming libraries exist for all platforms to accomplish this in the batch browser software, and all web servers also have this capability. The batch browser and the Web server are the two software components used to exchange X12 and Flat Files in the current GISB standard.

7.1.6 Interactive Processing

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

Sandia 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.

Sandia 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.

GISB Response: We concur with the finding and with the analysis. We would implement the recommendation separately for the functions addressed. The GISB response to this item is presented in three parts – the response applicable to informational postings, the response applicable to customer activities web sites, and the response applicable to flat files.

For Informational Postings: Informational Postings have always been considered information available to the public at large. Therefore, GISB standards have intentionally not imposed any security requirements for this data category. Since this information is intended for the public, an authentication mechanism (such as a logon) is not imposed. By not encrypting this data, GISB recognizes that it is vulnerable to an interception of the message with possible alteration of its content prior to it being viewed by the requestor. However the risk of such interception and modification is low compared to the effort required to do so. GISB could apply SSL encryption to this content to prevent this possibility, but it should noted that this will have a slight adverse affect on response time. Digitally signing this “display only” content, if possible, would have no value as the Web browser has no mechanism to utilize the attached signature.

GISB Responses to the Sandia Surety Assessment Findings:

GISB appreciates Sandia's recommendation, but does not at this time plan to take any action. As described above, the resources required to implement the recommendation are significant, and the risk assessed is minimal**.** Because of the unlikely event of an interception and modification of content, the cost to implement security measures to prevent such interception, and the barriers to easy access by the public that the security measures would impose, GISB at this time will not implement the security measures of PGP signatures for interactive processing of transactions under SSL encryption protection for the Informational Posting Web sites.

For Customer Activities Web sites: For Customer Activities Web sites, as noted in Sandia's report, GISB standards already call for applying encryption to Customer Activities data, and moreover, the GISB Standard No. 4.3.61 has been changed to refer to 128-bit encryption only (see finding 7.1.7). Sandia also suggests applying a digital signature to this data. A digital signature provides for non-repudiation. This means that the source of the transaction is provable and tamper-proof. Sandia further suggests using PGP with its ability to digitally sign what is on the clipboard. It is acknowledged that Sandia's recommendation suggests the best-known way to deliver non-repudiation. This would require that the browser contain code to write and read content to and from the clipboard, which appears to be supported with the most recent versions of IE and Navigator. It should be noted, however, that the user could disable pasting via script in IE, and possibly with Navigator. GISB's standard also allows use of the ICA protocol (otherwise known as Windows Terminal Server), which moves screen images to the client but the data entry form is actually running on the server machine, not the client. In this case, there is no way for the user on the client side to apply a digital signature using its private key.

Using PGP for digital signatures creates a considerable administrative burden as well since the trading partners would have to maintain, in many cases, a very large number of public keys. PGP keys are often exchanged using diskettes and the US Mail since use of email can be an insecure key exchange mechanism. There may be performance issues as the size of the PGP key ring grows to be very large. As we support an expiration period for these keys, the administrative task may grow even more. Of course, use of PGP by every on-line user means that they must purchase the PGP software and it must run on their desktop. This may affect sites that attempt to achieve a standard configuration and minimal client-side software for their users. Additionally, it creates a training requirement for the users.

All in all, the recommendation to use digital signatures is not implementable for those companies using the ICA protocol, and is costly for others. As an alternative, the browsers can provide for signing of Web forms using a certificate. A check with Microsoft revealed that IE 5.5 does not have this capability, which disallows this alternative as the GISB standards are required to work using either IE or Navigator browsers.

It appears that GISB will be unable to provide for non-repudiation by applying a digital signature to an interactive transaction. Disallowing the ICA protocol may make this more possible but it is still burdensome, at best, to implement this feature. It is suggested that we forego this until such time as a more practical approach is possible.

The risk of not implementing digital signatures is offset by the checks and balances that already exist for the natural gas transactions. For example, scheduled quantities transactions are sent after the nominations have been processed, and confirmations, both upstream and downstream are sent, so that use of confirmations for a variety of sources should minimize the risk of foul play as a result of no digital signature. Moreover, with GISB standards, the risk is of a commercial nature instead of physical impairment. If the digital signature technology were readily available, we would use it – but the exposure right now is not great enough to warrant the expense and resources to implement digital signatures and remove the ICA protocol as a choice that GISB standards currently allow. GISB will continue to look for ways to implement these securities when they become more mainstream and cost effective.

As described in the above discussion, GISB appreciates Sandia's recommendation and has taken steps to implement the SSL 128-bit encryption, but does not at this time plan to take any action on the recommendation regarding digital signatures. As described above, the resources required to implement the digital signature recommendation are significant, would require companies to relinquish the use the ICA protocol, and the risk assessed is minimal**.** Because there are checks and balances for a variety of sources to minimize the risk, the cost to implement digital signatures, and the reduction in the protocol choices that a company currently has, GISB at this time will not implement the security measures of PGP digital signatures for interactive processing of transactions for the Customer Activities Web sites.

For interactive flat files: The Interactive Flat File mechanism allows the user to construct a comma-separated-value (CSV) file using software such as a spreadsheet and then upload it using a Web browser. GISB supports the use 128-bit SSL encryption to protect this data from viewing or alteration (see finding 7.1.7, GISB standard no. 4.3.61).

Because the uploaded transaction is in the form of a file, it is possible for the user to apply a digital signature to the file after its creation. The same administrative issues as described the discussion on the Customer Activities Web sites apply also to interactive flat files. That is, there is the potential to have to maintain a large number of PGP public keys. However, as a practical matter, there appear to be very few users of this particular EDM mechanism, which reduces the administrative burden. Of course, the user would still be required to purchase and install the PGP client on the desktop and there would still be a training requirement. However, there appears to be little to be gained by having this capability for this particular on-line user while most on-line users would not have the capability.

Checks and balances already exist for the natural gas transactions such as scheduled quantities after the nominations have been processed, and confirmations, both upstream and downstream – so that the risk of foul play as a result of no digital signature is minimized. With GISB standards, the risk is of a commercial nature instead of physical impairment. If the digital signature technology were readily available, we would use it – but the exposure right now is not great enough to warrant the expense and resources to implement digital signatures. For the above reasons, GISB standards will implement 128-bit SSL encryption but forego implementing digital signature for interactive flat files. GISB will continue to look for ways to implement digital signatures as they become more mainstream and cost effective.

7.1.7 Secure Socket Layer (SSL)

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

Sandia 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.

Sandia 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.

GISB Response: We concur with the finding, the analysis and the recommendation. GISB standard 4.3.61 and 4.3.83 will be modified to:

4.3.61 ~~At a minimum,~~ ~~d~~Data communications for Customer Activities Web sites should utilize 128~~40~~-bit encryption. ~~Where possible, 128-bit encryption is recommended.~~

4.3.83 For interactive Flat File EDM, 128~~40~~-bit Secure Sockets Layer (SSL) encryption should be used. ~~Where possible, 128-bit SSL encrpytion is strongly recommended.~~

7.1.8 Basic Authentication

Sandia Finding: 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.

Sandia 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.

Sandia 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.”

GISB Response: We concur with the finding, analysis and recommendation. The sentence “Those companies who wish to conduct business across the Internet in an unsecure fashion may do so by mutual agreement” will be removed from the EDM Implementation Guide Section of Security Requirements.

7.1.9 Security Standards

Sandia Finding: 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.

Sandia 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.

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

GISB Response: GISB concurs with the finding and the analysis, and applies the recommendation differently to the different types of transactions: informational postings, customer activities web sites, interactive flat files, and ANSI ASC X12 EDI. For ANSI ASC X12 EDI,

7.1.10 Using a Web Server

Sandia Finding: 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.

Sandia 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.

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

GISB Response:

7.1.11 Web Access Ports

Sandia Finding: 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.

Sandia 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.

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

GISB Response: Response to be provided by the Future Technology Task Force.

7.1.12 Message replay attacks

Sandia Finding: Message replay is not addressed in the standards.

Sandia 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.

Sandia 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.

7.1.12 **GISB Response:** We concur with the finding that GISB EDM may be susceptible to replay attacks. However, the adoption by GISB of SSL encryption for EDM messages

(see item 7.1.5) precludes the interception of the message by a third party and replaying it repeatedly to destination server - a "deep denial of service" attack. While this technique does not preclude the possibility of a replay attack from a "man-in-the-middle" (DNS spoofing), it does mitigate the most likely causes of replay attacks. In response, the “man-in-the-middle” attack is unlikely and would take significant resources to prevent. SSL encryption should provide adequate security.

GISB appreciates Sandia's recommendation, but does not at this time, plan to take action other than the SSL encryption. The resources required to implement the recommendation are significant, and the risk assessed is minimal. As more cost effective solutions become commercially available, this response will be revisited.

7.2 Recommendations for GISB Principles

7.2.1 Grouping of Principles

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

Sandia 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.

Sandia 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.

GISB Response: We concur with the finding and analysis, and the recommendation will be implemented by providing a cross reference in the EDM standards manual that groups the principles functionally. For example, the standards can be categorized to areas of application – batch processing, customer activities web site standards, informational posting standards, and general application to all areas. The standards categorization does not imply a renumbering, but rather a cross reference that could apply to both the standards manuals and the little standards books. The numbers would be preserved and the standards would not be combined.

GISB Responses to the Sandia Surety Assessment Findings:

7.2.2 Future Technology Model

Sandia Finding: 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.

Sandia 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.

Sandia 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.

GISB Response: Response to be provided by the Future Technology Task Force.

7.2.3 Principle 4.1.2

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

Sandia 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.

Sandia 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."

GISB Response: GISB appreciates Sandia's recommendation, but does not at this time, plan to take any action. The resources required to implement the recommendation are significant, and the risk assessed is minimal.

7.2.4 Principle 4.1.6

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

Sandia 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.

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

GISB Response: GISB appreciates Sandia's recommendation, but does not at this time, plan to take any action. The resources required to implement the recommendation are significant, and the risk assessed is minimal.

7.2.5 Principle 4.1.8

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

Sandia 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.

Sandia 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.

GISB Response: GISB appreciates Sandia's recommendation, but does not at this time, plan to take any action. The resources required to implement the recommendation are significant, and the risk assessed is minimal.

7.2.6 Principle 4.1.15

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

Sandia 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.

Sandia 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."

GISB Response:

7.2.7 Principle 4.1.16, Principle 4.1.17 and Principle 4.1.19.

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

Sandia 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.

Sandia 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."

GISB Response: GISB appreciates Sandia's recommendation, but does not at this time, plan to take any action. The resources required to implement the recommendation are significant, and the risk assessed is minimal.

7.3 Recommendations for GISB Standards

7.3.1 Grouping of Standards

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

Sandia 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.

Sandia 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.

GISB Response: We concur with the finding and analysis, and the recommendation will be implemented by providing a cross reference in the EDM standards manual that groups the standards functionally. For example, the standards can be categorized to areas of application – batch processing, customer activities web site standards, informational posting standards, and general application to all areas. The standards categorization does not imply a renumbering, but rather a cross reference that could apply to both the standards manuals and the little standards books. The numbers would be preserved and the standards would not be combined.

7.3.2 Standard 4.3.4

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

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

Sandia 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?

GISB Response:

7.3.3 Standard 4.3.6

Sandia Finding: 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."

Sandia 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.

Sandia 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.

GISB Response:

7.3.4 Standard 4.3.8

Sandia Finding: 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."

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

Sandia 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.

GISB Response: We concur with the finding and analysis, and the recommendation. To implement the recommendation the following changes to the EDM Standard Manual and the EDM standards will be made:

- In the section titled "Related Standards", sub-section Hypertext Transfer Protocol (HTTP)" (page 44 of the PDF file),

  REPLACE:

  "HTTP has been in use by the World-Wide Web global information initiative since 1990. This specification reflects common usage of the protocol referred to as HTTP/1.0".

  WITH

  "HTTP has been in use by the World-Wide Web global information initiative since 1990. Appendix A of the Electronic Delivery Mechanism Related Standards manual contains a listing of the HTTP version(s) supported by GISB."

- And modify GISB Standard No. 4.3.8 to:

  4.3.8 The minimum acceptable protocol should be HTTP. All sending and receiving parties should be capable of sending and receiving the HTTP versions supported by GISB.

7.3.5 Standard 4.3.11

Sandia Finding: 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."

Sandia 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.

Sandia 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.

GISB Response: Response to be provided by the Future Technology Task Force.

7.3.6 Standard 4.3.15

Sandia Finding: 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."

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

Sandia 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

GISB Response: GISB appreciates Sandia's recommendation, but does not at this time, plan to take any action. The resources required to implement the recommendation are significant, and the risk assessed is minimal.

7.3.7 Consolidating like Standards

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

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

Sandia 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."

GISB Response: GISB appreciates Sandia's recommendation, but does not at this time, plan to take any action. The resources required to implement the recommendation are significant, and the risk assessed is minimal.

7.3.8 Standard 4.3.70

Sandia Finding: 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.”

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

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

GISB Response: We concur with the finding and analysis, and the recommendation. The recommendation will be implemented as follows:

GISB Responses to the Sandia Surety Assessment Findings:

- For the Sandia action item no. 7.3.8, the following wording be inserted into Appendix A of the EDM manual immediately following the section titled "HTTP":
  "Allowable TCP Ports (not UDP ports)
  HTTP 80, 5713, 6112, 6304, 6874, 7403
  SSL 443
  ICA. 1494
  RMI(Java.) 1099-1100
  Java. Telnet 31415
  TCP Optional 8001-8020**
  Allowable UDP Ports (not TCP ports)
  Secure ICA 1604
  **The reservation of 20 optional ports was to provide room for implementations such as DCE, IIOP, and load balancing implementations. TSPs should endeavor to minimize the usage of these ports."

- Subsequent to the change above the following changes to the EDM standards manual will also be required[1]:

  Page 20:
  Remove the text starting with "Allowable" and ending with "1604" .
  Insert "See Appendix A for a list of allowable TCP ports." as the last sentence of the first paragraph of the section titled "TCP Communications".

  Page 21 (at top):
  Remove the text associated with the "**" footnote

  Page 37, within the text for standard 4.3.70:
  Replace "in the Appendix" with "in Appendix A".
  Insert a "." after the word Manual and remove all the text after "Manual."

  Page 63(at bottom):
  REPLACE
  "The HTTP Server should be configured as port 80. If port 80 is not available, use one of the five recommended alternate ports: 5713, 6112, 6304, 6874, 7403."
  WITH
  “The HTTP Server should be configured to use one of the allowable TCP ports listed in Appendix A."

  Page 89:
  REPLACE

[1] NOTE: All page number references relate to the PDF page number of the EDM document.

"The HTTP Server or the server side application should be configured as port 80. If port 80 is not available, use one of the following recommended alternate TCP ports :

- HTTP 80, 5713, 6112, 6304, 6874, 7403
- SSL 443
- ICA 1494
- RMI (JAVA) 1099-1100
- JAVA Telnet 31415
- TCP Optional 8001-8020

Allowable UDP Ports (not TCP ports)

- Secure ICA 1604"

WITH

"A GISB EDM compliant Server should be configured to use one of the allowable TCP ports listed in Appendix A."

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

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

Sandia 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.

Sandia 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.

GISB Response: GISB appreciates Sandia's recommendation, but does not at this time, plan to take any action. The resources required to implement the recommendation are significant, and the risk assessed is minimal.

7.4.2 Definitions and Acronyms

Sandia Finding: 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.

Sandia 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.

Sandia 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".

GISB Response: GISB appreciates Sandia's recommendation, but does not at this time, plan to take any action. The resources required to implement the recommendation are significant, and the risk assessed is minimal.

7.4.3 Web Pages

Sandia Finding: 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.

Sandia 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.

Sandia 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.

GISB Response: We concur with the finding and analysis, and we appreciate Sandia's recommendation, but do not at this time, plan to take any action. The resources required to implement the recommendation are significant, and the risk assessed is minimal. Printed examples of formatting, layout and common look and feel are provided within the EDM standards manual.

7.4.4 Reference Guide Section

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

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

Sandia 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.

GISB Response:

7.4.5 GISB EDM document compatibility

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

Sandia 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.

Sandia 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.

GISB Response: We concur with the finding, the analysis and the recommendation. To implement the recommendation, we are creating a new principle:

4.1.X Trading Partners should mutually select and utilize a version of the GISB EDM standards under which to operate. Trading Partners should also mutually agree to adopt later versions of the GISB EDM standards, as needed.

7.4.6 Consistency of Terms

Sandia Finding: 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.

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

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

GISB Response: We concur with the finding and analysis, and the recommendation. The EDM Committee has looked for instances where the phrase "client configuration standard" occurs in the EDM Manual. A search identified only one instance of this in the EDM Manual, in the section titled "Technical Implementation - Interactive FF/EDM" under the sub-title "Security" and heading "Encryption." We will change the applicable paragraph as shown:

Encryption

"Standard 4.3.83 calls for the use of 40-bit encryption using Secure Socket Layer (SSL) technology. SSL is accomplished by obtaining a certificate from providers and using Web servers capable of using these certificates ~~to accomplish SSL~~. The ~~standard~~ browsers specified in the Standard Client Configuration ~~standard~~ are known to be able to handle SSL mechanisms. Any pages to be protected with SSL need to be invoked with the HTTPS protocol by using "https" versus "http" as part of the hyperlink (HREF) name. Note that this means using a Fully Qualified versus Relative link name. This, in turn, causes a new DNS lookup from the browser. When the hostname is provided by more than one machine, this may result in the request being sent to a different machine. This would only cause problems where necessary state information is being maintained in the memory of the Web server's machine."

With this change, GISB believes it has identified and corrected all inconsistent wording and usage in the EDM manual.

7.4.7 Clarify Encryption

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

Sandia 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.

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

GISB Response: Response to be provided by the Future Technology Task Force.

7.4.8 Compliance Statement

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

Sandia 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".

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

GISB Response: We concur with the finding that security choices were available in version 1.4. Specifically, GISB Standard No. 4.3.61 references a requirement to use 40-bit encryption for Customer Activities Web Sites with a strong recommendation to use 128-bit encryption where possible. To address this finding, this standard has been modified to refer to 128-bit encryption only. As such, there is no longer a security choice present in any of the standards that would necessitate specific titles for compliance levels.

GISB Responses to the Sandia Surety Assessment Findings:

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.

GISB Responses to the Sandia Surety Assessment Findings:

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.

GISB Responses to the Sandia Surety Assessment Findings: