Gas Industry Standards Board
1100 Louisiana, Suite 3625, Houston, Texas 77002
Phone: (713) 356-0060, Fax: (713) 356-0067, E-mail: gisb@aol.com
Home Page: www.gisb.org

TO:	GISB EDM Subcommittee Participants & Posting for Interested Industry Participants
FROM:	Rae McQuade, Executive Director, GISB Dick Brooks, Co-Chairman, GISB EDM Subcommittee Leigh Spangler, Co-Chairman, GISB EDM Subcommittee
RE:	Final Minutes from the GISB EDM Subcommittee Meeting
DATE:	April 12, 2001

GAS INDUSTRY STANDARDS BOARD

GISB EDM SUBCOMMITTEE MEETING

Conference Call: 2:00 p.m. to 4:00 p.m., April 12, 2001

FINAL MINUTES

I. Administrative

Mr. Spangler welcomed participants. Ms. McQuade read the roll call and gave the antitrust charge. The agenda was adopted as drafted. The draft minutes of March 30 were adopted with modifications made in the meeting.

II. Sandia Report Action Plan—Items Not Yet Discussed

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.

Discussion:

Mr. Keisler discussed the work paper presented by Mr. Hamilton:

Many of the ANSI X12 standards are not specified or recommended by GISB including X12.58. It would be inconsistent for GISB to document a standard that it does not specify or recommend. Because X12.58 is not a GISB recommendation no additional information is needed in Appendix A, Tab 10. To emphasize this fact, the following proposal should eliminate any ambiguity on how X12.58 relates to any GISB standard or recommendation.

Mr. Hamilton joined the call and reiterated the above comment.

Proposed response:

Change the wording under the Frequently Asked Questions last paragraph on page 26 to read:

Change From:

Both encryption methods are supported and do not conflict with each other. The use of PGP and X12.58 encryption must be specified in the Trading Partner Agreement.

To:

The use of internal encryption such as X12.58 is outside the scope of the GISB encryption standards.

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 strategies.

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 also be encrypted 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. To support this recommendation, the following standards will be added:

4.3.z: For EDI/EDM, 128-bit Secure Socket Layer (SSL) encryption should be used.

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.~~

Discussion:

Mr. Brooks and Mr. Lehn provided additional information to augment the response in 7.1.5 and 7.1.7. The response allows for the support of private certification authorities and "self signed" certificates. The response does not require that a company purchase a certificate from a third party.

III. Review of the Audit Report

In the review, a lack of time zone identifier in the response to 7.1.2 has caused some problems. Mr. Brooks will provide a request. Should the request be acted on and implemented where a time zone should be identified, it would not change GISB Standard No. 4.3.10, as shown in the GISB response below:

> **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.

The report was also changed for the response to Sandia Issue No. 7.1.5 to add a standard:

4.3.z For EDI/EDM, 128-bit Secure Socket Layer (SSL) encryption should be used.

The response to Sandia Issue No. 7.1.7 was changed to reflect use of 128-bit encryption using SSL.

IV. Assignments and Next Agenda

The next meeting will be a conference call to review the draft report and recommendation. It will be held on Thursday, May 17 from 2:00 to 4:00 pm central.

V. Adjournment

The meeting adjourned at 3:30 p.m.

VI. Attendees

Name	Company
SERVICES SEGMENT:	
Gina McMahon	BTUWatch.com
Leigh Spangler	Latitude Technologies
Dick Brooks	Group 8760

PIPELINE SEGMENT:

Jim Keisler	Williams Gas Pipeline
Terry Lehn	Enron Transportation Services
Theresa Hess	Enron Transportation Services

ADMINSTRATIVE:

Rae McQuade	GISB
JoAnn Garcia	GISB