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:	March 16, 2001

GAS INDUSTRY STANDARDS BOARD

GISB EDM SUBCOMMITTEE MEETING

Conference Call: 9:00 p.m. to 12:00 p.m., March 16, 2001

FINAL MINUTES

I. Administrative

Mr. Spangler welcomed participants. Ms. McQuade read the roll call and gave the antitrust charge. The agenda was adopted with an addition to add NAI relationship with GISB. The draft minutes of February 28 were adopted with modifications.

II. Sandia Report Action Plan—Items Not Yet Discussed

The group started the meeting with the reports from those assignments of the last meeting:

7.4.6 Modify the EDM Manual to provide consistency of terms – for example, "standard client configuration" versus "client configuration standard."

Discussion: There was a question on if the difference in terms is a substantive change. It was determined to review the EDM standards manual to determine if the change can be made and if there are substantive issues.

Assignment: Mr. Keisler agreed to investigate this item.

7.4.8 Absence of a compliance statement.

Discussion: When there are options offered in the standard, Sandia recommended that the standards annotate the options with the level provided for each option (weak – such as 40-bit key encryption, to strong – such as 128-bit key encryption). The recommendation could be part of the GISB certification – providing various levels of certification depending the options chosen. It was further noted that options in a standard would no longer be present as the one standard offering options is being changed to reflect only the highest option.

Assignment: No assignment. The response will correspond to the above discussion. A compliance statement is no longer needed as the standard that refers to options has been changed so that no options exist. The standard that refers to both 40-bit and 128-bit key encryption has been changed to refer to 128-bit key encryption only.

III. Sandia Report Action Plan—Work Papers Provided

7.1.1 Work paper provided by Mr. Keisler was discussed. Since the Trading Partner Agreement (TPA) lays out which trading partner will perform what function and how Internet EDM will be accomplished (including such items as user names and passwords), the TPA should be protected from unauthorized exposure. Sandia

recommended that each trading partner should protect the TPA as a proprietary company document.

Proposed GISB Response: The EDM Committee will ask the Contracts Committee to add the following note 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."

Discussion: All on the call agreed with the concept represented in the proposed language.

7.1.12 A work paper provided by Mr. Spangler was discussed regarding message replay attacks. The Sandia concern is that GISB EDM may be susceptible to replay attacks by a third party intercepting a message and replaying it repeatedly to destination server - a "deep denial of service" attack.

A proposed GISB Response was provided: 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 for replay. 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.

Discussion: The "man-in-the-middle" attack is unlikely and would take significant resources to prevent. SSL encryption should provide adequate security.

7.4.5 A work paper was provided by Mr. Spangler regarding GISB EDM document compatibility. The Sandia concern is that version compatibility is not discussed in the GISB standards or the TPA. There was a suggestion of revising the TPA and including statements about backward compatibility.

A proposed GISB Response: Create GISB 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."

7.2.1 A work paper was provided by Mr. Spangler regarding a grouping of principles. The Sandia concern is that principles should be (re)organized by topic, instead of chronologically.

A proposed GISB response is that while GISB recognizes the chronologically organization of the Principles may appear arbitrary to the unknowing reader, the organization of Tab 4 is consistent with the organization of all GISB standards.

Discussion: There may be concern on to which areas the standards apply – batch processing, customer activities web site standards, informational posting standards, and general application to all areas. If the standards were categorized, it would not mean a renumbering, but rather a cross reference that could apply to both the standards manuals and the little standards books.

Assignment: Categories should be defined and then the standards should be assigned to each of the categories. Ms. McQuade will put a work paper together and provide it to Leigh Spangler based on the course material taught, and the proposed GISB response will be modified to reflect that GISB will add a cross reference.

7.1.5 A work paper provided by Mr. Lehn described Sandia issue no. 7.1.5, EDI & Batch Flat File GISB Standard no. 4. 3.15, recommending 128-bit encryption security.

Discussion: EDI & Batch Flat File – Sandia recommends that we encrypt the HTTP

message to ensure that the user id and password are encrypted. Discussion at the 2-14-2001 meeting yielded general agreement that we should take Sandia's recommendation. We also agreed that this should be accomplished using Secure Sockets Layer (SSL) with 128-bit encryption. It is believed that programming libraries exist for all platforms to accomplish this in the batch browser software. It is also believed that all Web servers are capable of this. The batch browser and the Web server are the two software components used to exchange X12 and Flat Files in the current GISB standard. Those in the meeting were to follow-up with their technical teams to confirm this in their companies. We will rely on any feedback from the greater GISB membership when our recommendations are made available for comment to have confidence that this will work for all.

A proposed GISB Response: Use SSL with 128-bit encryption for X12 and flat files.

7.1.6 A work paper provided by Mr. Lehn described Sandia issue no 7.1.6, regarding informational postings described in GISB Standard No. 4.3.20.

Discussion: Sandia's report does not seem to distinguish Informational Postings from Customer Activities. They simply refer to "Interactive Processing" and "transactions". Participants in the 2-14-2001 meeting agreed that we should distinguish between Informational Postings and Customer Activities in our response to Sandia's report. We also agreed that 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) should not be imposed. By not encrypting this data, we are vulnerable to someone intercepting the message and altering its content prior to it being viewed by the requestor. This requires a fair amount of effort to accomplish. We 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.

A proposed GISB Response: Informational Postings are designed for ease of access by the public at large. As such, no security was specified.

7.1.6 and 7.1.7 EBB (Customer Activities) 4.3.60, 4.3.61 Secure (7.1.6, 7.1.7) Secure using 128-bit encryption but no digital signature

Discussion: Customer Activities – As noted in Sandia's report, GISB standards already call for applying encryption to Customer Activities data. However, the current standard makes 128-bit encryption optional. Discussion in the 2-14-2001 meeting favored making 128-bit encryption standard. However, 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. They suggest 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. This 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 (not sure about Navigator). However, our current standard allows use of the ICA protocol (AKA Windows Terminal Server). This protocol 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. (It is likely that Sandia was unaware of the implication of using this protocol). Using PGP creates a considerable administrative burden as well since the trading partners (especially, TSPs) 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 are also considering 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, this approach appears to be unfeasible (especially due to the ICA problem). Another alternative is the possibility that the browsers provide for signing of Web forms using a certificate. A check with Microsoft revealed that even IE 5.5 does not have this capability which means this alternative is not available since it must work on both IE and Navigator (did not investigate Navigator as the point is moot). It appears that we 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.

Discussion: 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. GISB will continue to look for ways to implement these securities when they become more mainstream and cost effective.

A proposed GISB Response: For the Customer Activities Web Sites, secure using 128-bit encryption but no digital signature.

7.1.6 and 7.1.7 Interactive Flat File 4.3.83, 4.3.84 Secure (7.1.6, 7.1.7) Secure using 128-bit encryption but no digital signature

Discussion: Interactive Flat File – 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. It makes sense to utilize 128-bit SSL encryption to protect this data from viewing or alteration. 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 in 2c above apply here. 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. For this reason, it suggested that we implement 128-bit SSL encryption but forego implementing digital signature for this type of EDM.

Discussion: 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. GISB will continue to look

for ways to implement these securities when they become more mainstream and cost effective.

A proposed GISB Response: For the interactive flat files, secure using 128-bit encryption but no digital signature

7.1.4 CAR—4.3.20 CAR—Secure (7.1.4) CAR—Non-secure—present blocking legitimate users issue to BPS.

Discussion: Central Address Repository (CAR) - Sandia suggests that we protect the CAR using both SSL encryption and a logon authentication. As the CAR data is read-only, this imposes a requirement only on GISB's Web site. It is relatively easy to implement, especially if there is only one userid and password to be used by all GISB members. The GISB office, via a mailing or the annual meeting, could provide this information. The only question is whether this would have the effect of unintentionally blocking access for legitimate users. This question should be addressed by GISB.

Discussion: The cyberwar scenarios are an unlikely threat, and moreover, this is information to ehich the public at large should have convenient and easy access.

A proposed GISB Response: 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. As such, GISB does not recommend that security be implemented for the Central Address Repository.

III. Assignments

Date Assigned	Items	To be Addressed By	Addressed
02/28	7.1.01	Jim Keisler	Yes
02/14	7.1.03	Dick Brooks	Yes
02/28	7.1.04	Terry Lehn	Yes
02/14	7.1.05	Terry Lehn	Yes
02/14	7.1.06	Terry Lehn	Yes
02/14	7.1.07	Terry Lehn	Yes
02/28	7.1.08		Yes
02/14	7.1.09	Terry Lehn	Yes
	7.1.10		
02/14	7.1.12	Leigh Spangler	Yes
02/28	7.2.01	Leigh Spangler	Yes
02/28	7.2.03	Dick Brooks	No
02/28	7.2.04	Dick Brooks	No
02/28	7.2.05	Dick Brooks	No
02/28	7.2.06	Dick Brooks	Yes
02/28	7.2.07	Dick Brooks	No
02/28	7.3.01	Dick Brooks	No

02/28	7.3.02		Yes
02/28	7.3.03		Yes
02/28	7.3.04	Dick Brooks	No
02/28	7.3.06	Dick Brooks	No
02/28	7.3.07	Dick Brooks	No
02/28	7.3.08	Dick Brooks	No
02/28	7.4.01	Dick Brooks	No
02/28	7.4.02	Dick Brooks	No
02/28	7.4.03	GISB Office	No
02/28	7.4.04	Richard Hamilton	No
02/14	7.4.05	Leigh Spangler	Yes
03/16	7.4.06	Jim Keisler	No
03/16	7.4.08	Addressed in Meeting	Yes

IV. Network Associates

A conference call will be scheduled for Mr. Spangler, Mr. Brooks and Ms. McQuade to discuss open issues with Network Associates regarding PGP applications. A summary of items identified by several participants will be prepared by Ms. McQuade prior to the conference call.

V. Next Agenda

The next meeting will be a conference call to continue work on the action plan, and is scheduled for March 30 from 9:00 a.m. to noon central time – which will take place of the previously announced face-to-face meeting on March 30. The face-to-face meeting was cancelled because conceptual responses have not been determined for all of the action items assigned to EDM.

VI. Adjournment

The meeting adjourned at 11:00 a.m.

VII. Attendees

Name	Company
SERVICES SEGMENT:	
Gina McMahon	BTUWatch.com
Leigh Spangler	Latitude Technologies
PIPELINE SEGMENT:	
Jim Keisler	Williams Gas Pipeline
Terry Lehn	Enron Transportation Services

LDC SEGMENT:

Mike Shahan	Dominion

ADMINSTRATIVE:

Rae McQuade	GISB