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

GAS INDUSTRY STANDARDS BOARD

SANDIA PLAN

Directive

The Board of Directors approved the GISB 2001 Annual Plan to address the Sandia National Laboratories Report. The GISB Annual Plan identifies the following directive:

6. Develop plan to consider surety assessment recommendations based on the Sandia National Laboratories. Implement those that are determined needed, including changes to existing GISB standards.

Plan Description

Sandia National Laboratories, under the guidance of the Department of Energy prepared and assessment report of the GISB EDM standards. The report drew the conclusions that:

> "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."

The report also specified several enhancements to GISB standards to provide additional protection. The plan should address these recommended enhancements and prepare a recommendation for industry comment, and for the consideration of the Executive Committee.

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

GAS INDUSTRY STANDARDS BOARD
SANDIA ACTION PLAN PREPARED ON _____

Item Description	Completion
Review each recommendation in the Sandia Report, and determine responses and/or recommendation for:	
1 Collect metrics for analysis of security and reliability measures.	
2 Recommendations for Security Issues:	
7.1.1 Trading Partners should protect the TPA as a proprietary document.	
7.1.2 Require clients to acquire time-of-day from the server and check hat time against their on reference, with notification to the use of discrepancies higher than a specified threshold.	
7.1.3 Manage keys with a set expiration date.	
7.1.4 Protect the CAR using SSL and basic authentication.	
7.1.5 Encrypt batch processing of requests and responses messages with SSL.	
7.1.6 PGP signatures should be requires for interactive processing of transactions under SSL encryption protection.	
7.1.7 128 bit SSL should be cited on GISB Standard Nos. 4.3.61 and 4.3.83, and all client authentication should be done under the protection of 128 bit SSL.	
7.1.8 Remove the statement "Those companies who wish to conduct business across the Internet in an unsecure fashion mat do so by mutual agreement."	
7.1.9 Require the use of strong encryption and strong authentication on all transactions.	
7.1.10 Establish SSL session prior to the HTTP Post process to protect the userID, password and any header information.	
7.1.11 Use standard TCP ports for web servers.	
7.1.12 Address message replay in the standard to disallow replay attacks.	
3 Recommendations for GISB Standards in the EDM Manuals:	
7.2.1 Change the grouping of principles from chronologically in tab 4 to categories.	
7.2.2 Enhance the Future Technology Model diagram, (GISB Standard No. 7.2.2).	

Item	Description	Completion
7.2.3	Reword GISB Standard No. 4.1.2 to clarify its meaning.	
7.2.4	Reword GISB Standard No. 4.1.6 to clarify its meaning.	
7.2.5	Move GISB Standard No. 4.1.8 within the governance principles.	
7.2.6	Revise GISB Standard No. 4.1.15 to include concepts in GISB Standard No. 4.3.15.	
7.2.7	Consolidate GISB Standard Nos. 4.1.16, 4.1.17 and 4.1.19 with clarifying language.	
4	Recommendations for GISB Standards in the EDM Manuals:	
7.3.1	Change the grouping of standards from chronologically in tab 4 to categories.	
7.3.2	Provide more information on GISB Standard No. 4.3.4 – specifically who should retain information, the volume of the information, security concerns were noted among others.	
7.3.3	GISB Standard 4.3.6 should be more specific – particularly the phrase "within a reasonable amount of time."	
7.3.4	State which version of HTTP should be used in GISB Standard No. 4.3.8.	
7.3.5	Reliance on IP addressed in GISB Standard No. 4.3.11 allows for "spoofing." A mechanism should be put in place to "close the loop."	
7.3.6	Break GISB Standard No. 4.3.15 into parts addressing server authentcation, SSL encryption and PGP 2.6 or compatable.	
7.3.7	Consolidate GISB Standard Nos. 4.3.36, 4.3.37 and 4.3.38 as they all address similar internet concerns.	
7.3.8	Correct the reference of GISB Standard No. 4.3.70 from appendix to tab 4.	
5	For format and layout of the EDM standards manual:	
7.4.1	Change the page numbering scheme used in the manual, referencing the tab number in the page number -- for example, "Page 2-1" would be page 1 of tab 2.	
7.4.2	Reorder the materials in the EDM manual so that the definitions are presented first.	
7.4.3	Develop a sample or model web site including the layouts and concepts presented in Tab 8 of the EDM manual.	
7.4.4	Add Guideline Adoption Procedure and X12.58 encryption standard to the Reference Guide section (Appendix A, Tab 10) of the manual.	

	Item Description	Completion
	7.4.5 Both trading partners should support the same GISB EDM version for GISB EDM document compatibility.	
	7.4.6 Modify the EDM Manual to provide consistency of terms – for example, "standard client configuration" versus "client configuration standard."	
	7.4.7 Clarify where and how it is expected that the encryption take place in the process. Provide additional details on the encryption.	
	7.4.8 Absence of a compliance statement	
6	Determine response and/or recommendation to the following weaknesses identified by Sandia National Laboratories: 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.	
7	Prepare Recommendation Report and send out for industry comment.	
8	Present recommendation to the Executive Committee for consideration.	