

GISB FTTF Meeting
April 24, 2001
CMS – Houston, TX
***FINAL* Minutes**

- The FTTF meeting was called to order at 9:15, at CMS offices in Houston, TX, by the Chair, Mike Shahan

- The following were in attendance:
 - Mike Shahan Dominion-Peoples
 - John Smith Dominion Transmission
 - Gina McMahon BTU Watch
 - Joe Kardas NFGSC
 - Jim Keisler Williams Gas Pipeline
 - Richard Hamilton Williams Gas Pipeline
 - Dick Brooks Group 8760
 - Kim VanPelt CMS, PEPL

- Mike Shahan read the ‘GISB Anti-trust Statement’.

- An item was added to the published agenda to discuss potential impacts of migrating to new versions of JAVA. The Agenda was adopted as amended.

- Minutes from November 7, 2001 FTTF meeting were adopted as corrected.

Sandia Issues

- 7.1.11 Use standard TCP ports for web servers
 - This standard was originally developed to address certain companies ‘security concerns’ of using standard port 80. We agree that the use of these ports do not provide any additional security.
 - Some companies are still using these ports.
 - We don’t know of any conflicts.
 - We could try to register these ports with IANA to make them ‘standard’ ports.
 - The referenced GISB standards do not specifically reference ports. The specific ports are listed in the implementation guide.
 - FTTF’s recommendation:
 - FTTF agrees that there are no security benefits gained by using specified ports; however FTTF wants to retain the use of specified ports to provide administrative benefits due to their existing use.
 - GISB will investigate the possibility of registering all of the specified ports. This would eliminate the concern of potential conflicts with other services. The specified ports may already be registered to another service. (Richard Hamilton will report back to FTTF on the availability of these ports to register; what the

issues are if none of these ports are available; as well as what other ports may be available).

- 7.2.2 Enhance the Future Technology Model diagram
 - FTTF reviewed and discussed standard 4.1.1. We do not agree with the Sandia analysis that the model is an important diagram. The diagram had some benefit when the industry was transitioning from VANS to the Internet, but at this point provides more confusion than clarification. There are other diagrams in the implementation guide that provide a better depiction of the EDM flow. Specifically there is a 'Batch Flow Diagram'; 'Informational Postings EDM Flow Diagram'; flow diagram for EBB EDM, and flow diagram for IFF (Interactive Flat File).
 - FTTF does not agree with the Sandia recommendation. Instead we recommend that 4.1.1 be eliminated from the GISB standards.

- 7.3.4 State which version of HTTP should be used in GISB Standard No. 4.3.8.
 - This issue was addressed by EDM. FTTF concurs with EDM's response and has no additional comments.

- 7.3.5 Reliance on IP addresses in GISB Standard No. 4.3.11 allows for "spoofing." A mechanism should be put in place to "close the loop."
 - Only synchronous responses are sent back to the sending address. These responses do not contain any proprietary or 'business' information. Basically, these responses contain a time-stamp as an acknowledgement of receipt of the transaction. Spoofing of this transaction creates no business risk.
 - The Sandia analysis and recommendation does not account for the fact that basic authentication (userid and password) are required. SSL makes this transaction even more secure and more difficult, if not impossible, to spoof.
 - FTTF appreciates Sandia's recommendation, but does not agree at this time that any action is required. Spoofing, as defined here by Sandia, would create no business risk since we use basic authentication and PGP encryption and any resulting answer set would be sent to the registered URL, not the address of the requesting transaction. EDM has made a recommendation that SSL be required to protect the userid and password in response to other Sandia findings (see response to Sandia issue 7.1.5).

- 7.3.6 Break GISB Standard No. 4.3.15 into parts addressing server authentication, SSL encryption and PGP 2.6 or compatible.
 - This issue was addressed by EDM. FTTF concurs with EDM's response and has no additional comments.

- 7.3.7 Consolidate GISB Standard Nos. 4.3.36, 4.3.37 and 4.3.38 as they all address similar internet concerns.

- This issue was addressed by EDM. FTTF concurs with EDM's response and has no additional comments.
- 7.4.7 Clarify where and how it is expected that the encryption take place in the process. Provide additional details on the encryption.
 - FTTF agrees with Sandia's discussion and analysis.
 - FTTF recommends making the following addition to the EDM manual – "Encryption/Digital Signature" within the "SECURITY" section:
 - Encryption and signatures are applied to files already translated to a GISB standard data format, and before the data is sent to the batch browser.

Annual review of EDM manual minimums and configurations

- The group discussed, and agreed, on the following recommendations. It was also discussed that we should not yet forward these recommendations to the EC to be processed. Instead, we should make these recommendations into a FTTF work paper that can be reviewed and changed throughout the year with a final review at year-end, and submission to the EC to be processed in time to be included in the 2002 publication. The FTTF feels that there is too much of a time lapse between now and the next publication and some of the recommendations made today may no longer be valid then, and additional changes may be identified by then.
 - Client for Customer Activity Website (Appendix C)
 - Change from ≥ 300 MHz to ≥ 500 MHz
 - Change from ≥ 96 MB to ≥ 256 MB
 - Add LINUX and Windows ME to example OS
 - We recommend that the date be removed from the Appendix C headings
 - Client for Informational Posting Website (Appendix D)
 - We recommend that the date be removed from the Appendix D headings
 - Changed from 90 MHz to ≥ 200 MHz (I can't find this in the document)
 - Changed from 32MB to 128MB
 - HTTP version
 - Currently reference HTTP 1.0
 - HTTP 1.1 is available and supports virtual hosting which some companies would like to use. The use of HTTP 1.1 would require a rewrite of batch browsers.
 - We recommend that all references to HTTP 1.0 be changed to HTTP 1.1
 - SSL to port 443
 - Dick wants to clarify that SSL is not restricted to port 443 but that SSL is allowable on any HTTP port. Change allowable TCP ports section: add HTTPS as well as HTTP and move 443 port up. Also add SMTP port 25 to list of allowable ports.

- Open PGP
 - Dick Brooks will develop a work paper on this issue.
- Compliance with 'GA' versions
 - With the new wording, providers of Customer Activity Websites should be at JAVA 1.2 and JAVA 1.3 soon (within 12 months of GA release). Some companies are ready to move to 1.3, but the plug-in will then conflict with those companies still using JAVA 1.1. All providers must comply with GISB standards so that users do not experience conflicts.

- Mike Shahan was elected as the Chairman of FTTF for the coming year.
- The date for the next FTTF meeting was set for Wednesday, May 9, 2001. This teleconference meeting will be to approve the minutes from today's meeting so the Sandia recommendation can be forwarded to EDM in order to be processed and submitted to the June EC meeting.
- The meeting was adjourned at 1:30 PM.