FTTF - Minimums and Versions
2001 Recommendations
To Become Effective in the 2002 Publications

- **Business Process and Practices—Overview—TCP Communications**

GISB Principle 4.1.37 and GISB Standard 4.3.70 restrict the TCP ports used as a standard for EDM communications. The usage of GISB standard ports may require modifications in the client-side firewall to allow for communications with the various service providers' EDM* implementations. Upon request, the TSP should indicate to their trading partners which specific TCP ports they will require to be opened to conduct electronic communication.

Allowable TCP Ports (not UDP ports)

HTTP HTTPS 80, 443, 5713, 6112, 6304, 6874, 7403
~~SSL 443~~
ICA® 1494
RMI(Java®) 1099-1100
Java® Telnet 31415
TCP Optional 8001-8020**
SMTP 25

Allowable UDP Ports (not TCP ports)

Secure ICA 1604

There are other technologies available that would require additional ports to be opened, such as FTP~~,~~ and Telnet~~, and SMTP~~. If and when GISB approves such technologies, FTTF will modify this list of allowable ports accordingly. The client-side firewall implementation and client browser settings should permit the downloading and installation of GISB approved plug-ins and modules. Please refer to the GISB defined Minimum Technical Characteristics for Accessing Customer Activities Web Sites for the listing of GISB approved plug-ins and modules.

These guidelines will be reviewed and updated by the Future Technology Task Force, at a minimum, by the spring of each year and presented to the GISB Executive Committee for adoption by the June meeting of that group.

*All GISB standard Internet communications
**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.

- **Business Process and Practices—Overview—Security**

Though many decisions as to overall security measures are left to each trading partner and their environment, several security measures were established as standards to ensure a minimum level of confidence in conducting business over the Internet and to provide some uniformity in the implementation of security. Four primary security aspects were considered as vital in providing the level of protection of transactions needed for gas industry commerce: data privacy, data integrity, authentication, and non-repudiation. The FTTF found that these concerns are addressed by the use of encryption and digital signature capability of the Pretty Good Privacy (PGP) security application. Any process used for encryption and decryption compatible with PGP 2.6 (using keys generated with the RSA algorithm) meets the minimum standard to be applied to files transmitted over the Internet. To prevent unwanted intruders from connecting to the Web sites, basic authentication is the required standard. Additional issues such as firewall security are discussed in the standards, but are considered implementation issues to be addressed by each organization.

- **Business Process and Practices—Standards--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.

- **Business Process and Practices—Standards--4.3.59**

Providers of Customer Activities Web sites should ensure that the site operates within the guidelines of the "Technical Characteristics of the Client Workstation" described in the Appendix of the Electronic Delivery Mechanism Related Standards Manual. This appendix, listing examples of hardware and software configurations that providers should meet, should be reviewed and updated by the Future Technology Task Force, at a minimum, by the spring of each year and presented to the GISB Executive Committee for adoption by the June meeting of that committee.

- **Related Standards—Hypertext Transfer Protocol (HTTP)**

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~~1".

- **Technical Implementation – Internet EDI/EDM & Batch FF/EDM—Server Specifications**

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.

- **Technical Implementation – Internet EDI/EDM and Batch FF/EDM—Server Specifications**

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.

- **Technical Implementation – Internet EDI/EDM and Batch FF/EDM—Security Requirements**

File encryption of the EDI is also selected as a security standard for transmission on the Internet. The encryption software is required to be compatible with PGP 2.6 or greater (using keys generated with the RSA algorithm). Those companies who wish to conduct business across the Internet in an unsecure fashion may do so by mutual agreement.

- **Technical Implementation – Internet EBB/EDM—Security—Encryption**

At a minimum, data communications for a 'Customer Activities' site should utilize 40-bit encryption. Where possible, 128-bit encryption is strongly recommended. This may be implemented through any of the following techniques:

- 40-bit SSL
- 40-bit RSA JAVA ® communications
- 40-bit secure ICA ®

Specific products should be reviewed prior to implementation for Year 2000 compliance.

- **Technical Implementation – Internet EBB/EDM—Server Specifications – Ports ***

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 HTTPS 80, 443, 5713, 6112, 6304, 6874, 7403
~~· SSL 443~~
· ICA ® 1494
· RMI (JAVA ®) 1099-1100
· JAVA ® Telnet 31415
· TCP Optional 8001-8020
· SMTP 25

Allowable UDP Ports (not TCP ports)

· Secure ICA 1604

Transportation Service Provider EDM implementations should minimize the number of outbound ports required to be opened on the client side firewall. Each time a server application requires another open port, it is potentially necessary for the users of that site to open yet another outbound port. An effort has been made to provide a limited number of these ports, and a user should be able to use any EDM site if all of these outbound ports have been provided.

FTTF - Minimums and Versions
2001 Recommendations
To Become Effective in the 2002 Publications

***** Technical implementations above represent a non-comprehensive set of choices which an implementer may use. This list in no way should be construed as an endorsement by GISB of any specific products. Other products supporting the technical implementation may be used.

- **Technical Implementation – Interactive FF/EDM—Security—Authentication**

Standard 4.3.84 calls for use of Basic Authentication. This is a standard part of the ~~HTTP 1.0~~HTTP 1.1 specification. Without use of encryption, this would be a clear text transmission of user id and password. To avoid this, merely protect the page from which the logon is invoked with Secure Sockets Layer encryption as described below. Note that where the user id and password information is maintained, it is different for
different Web environments. You may want to consider providing the ability for users to change their password.

- **Technical Implementation – Interactive FF/EDM—Security—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 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.

- **Appendix A – Reference Guide--HTTP**

The GISB EDM architecture is based on ~~HTTP 1.0~~HTTP 1.1, and all implementations should be compatible with this version.

W3C WorldWide Web Consortium. All aspects of HTTP, HTML, and other Web-related topics are documented at:
http://www.w3.org/pub/WWW/

General information regarding HTTP with basic terminology included are documented at:
http://www.w3.org/pub/WWW/Protocols/HTTP/1.0/spec.html

Syntax information for multipart can be found in IETF RFC1341 section 7.2. (www.ietf.org)

- **Appendix A – Reference Guide--HTML**

Before April 24, 1998, the recommended standard from the WorldWide Web Consortium was HTML 3.2. The specification for this standard can be found at:
http://www.w3.org/pub/WWW/TR/REC-html32.html

Effective April 24, 1998, the WorldWide Web Consortium has made a recommendation for HTML 4.0. Information on HTML 4.0 may be found at http://www.w3.org/TR/REC-html40/.

http://www.ncsa.uiuc.edu/General/Internet/WWW/HTMLPrimer.html

http://www.interlink-2000.com/guide-to-publishing-html.html

Special Edition Using HTML, Second Edition, Mark Brown, John Jung, and Tom Savola, Que Corporation, 1996.

FTTF - Minimums and Versions
2001 Recommendations
To Become Effective in the 2002 Publications

- **Appendix C Minimum ~~(??/??/????)~~ Technical Characteristics and Guidelines for the Customer Activities Web Site)**

Browser Characteristics (includes defined GISB current versions):

Features as supported by the latest generally available (GA) versions of both Netscape® 2 and Internet Explorer® . 3

within 6 months of such GA version becoming available, including –

Frames & Nested Frames
Tables & Nested Tables
HTML
Cookies
JavaScript
SSL 40-bit RSA Encryption
Style Sheets

Plug-ins (Generally Available (GA) versions within 12 months of such GA versions becoming available)

JAVA® 4
ActiveX® (Plug-in for Netscape®) 5
Independent Computer Architecture (ICA®) - Protocol used for remote control access to an application

Operating Systems:

Operating systems on a client workstation should be multithreaded and preemptive.

Hardware:

CPU >=~~300~~ 500 MHz
Memory >=~~96~~ 256 MB Physical
Display Resolution >=1024 x 768
Connection > =56 KB (v.90)

Example Configuration 1

Hardware:	CPU: P300 MHz or higher
	Memory: 96MB Physical
	Display Resolution: 1024 x 768
	Pointing Device with left and right click capability
Operating Systems:	
	Windows® 98 2
	Windows® ME
	Windows® NT 4.0
	Windows® 2000
	LINUX
Connection:	56KB (v.90) modem
	ISDN
	Direct Connect (T1, Fractional T1, etc.)
	DSL
	Cable-Modem
Browser:	Netscape® Communicator/Navigator
	Microsoft® Internet Explorer
Plug-ins:	JAVA®
	ActiveX® (Plug-in for Netscape®)
	ICA®

Memory - Users who want to have multiple applications or EBBs open simultaneously should consider more memory.

CPU Speed - Users should be aware that higher CPU speeds may result in better performance.

- **Appendix D--Minimal and Suggested ~~(??/??/????)~~ Technical Characteristics and Guidelines for the Developer and User of the Informational Postings Web Site)**

User technical characteristics provide specifications to the developer on the user environment for which the application will be designed and tested. Likewise, they will serve as guidelines to the user when purchasing the appropriate hardware and software to enable him/her to use the application.

Informational Postings Web Site User Technical Characteristics

	Minimal	Suggested ~~(??/??/????)~~
Connection Device:	28.8 KB	Direct Connect
Operating System:	Multi-threaded & Preemptive	
RAM:	~~32~~ 128 MB	>~~32~~ 128 MB
Browser Capabilities:	Cookies & JavaScript Frames & Nested Frames Tables & Nested Tables HTML 3.2	
Display Resolution:	800x600, 256 colors	16k colors

Definitions:

Minimal user technical characteristics –

The environment and components for which the Web site application is designed and tested. This should include:

- a client environment comprised only of characteristics listed above, and,
- support for all mandated functions in accessing Informational Postings

Suggested user technical characteristics –

Environment or components not required to perform all mandated functions in accessing Informational Postings, but could provide an enhanced user experience.

Examples of User Workstations Meeting Criteria of Informational Postings Web Site User Characteristics[1]

	Minimal	Suggested ~~(??/??/????)~~
Hardware:	Pentium® 200~~90~~MHz or equivalent	Pentium® 200MHz or greater [2]
RAM:	~~32~~ 128 MB	> ~~32~~ 128 MB
Communication Device:	28.8	Direct Connect ISDN Satellite 56 KB modem DSL Cable-Modem

FTTF - Minimums and Versions
2001 Recommendations
To Become Effective in the 2002 Publications

Monitor:	12" Laptop 15" Desktop	> 12" Laptop > 15" Desktop
Display Capabilities:	800 x 600 256 colors	> 800 x 600 > 256 colors
Operating System:	Windows® 95 System 7® Solaris® 2.5	Windows® 98 Windows® NT 4.0 [3] Solaris® 2.6 4 System 8® Windows 2000® Windows ME® LINIX
Browser:	Microsoft Internet Explorer® Netscape® Communicator	Microsoft Internet Explorer® Netscape® Communicator

Informational Postings Web Site Developer Technical Characteristics
User's environment supporting the above minimum characteristics should be able to access all GISB standardized features of Informational Postings Web Sites.

Any other Web technologies may be considered for use by the developer as long as they can be used by the client without requiring special actions including firewall rule changes, use of a specific browser, logons and downloads of special helper applications such as plug-ins, viewers or readers.