APPENDIX A - Reference Guide

CGI

An excellent source on CGI is a book entitled “Special Edition Using CGI” by Jeffrey Dwight and Michael Erwin.

Firewall Security

An excellent source which covers this topic in detail is a book entitled "Firewalls and Internet Security: Repelling the Wily Hacker" by William Cheswick and Steven Bellovin.

NAESB

NAESB Web Site: (http://www.naesb.org) Primary reference for natural gas industry standards

General NAESB WGQ FTTF Reference Page: (http://www.naesb.org/fttf.htm). This location provides pointers to samples and further documentation.

HTTP

The NAESB WGQ EDM architecture is based on 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/1.1/spec.html

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

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.

PGP Software

PGP is available for a variety of operating systems and platforms. For more information contact

Network Associates (http://www.nai.com)

OpenPGP Software

The IETF OpenPGP standard is available at http://www.ietf.org/rfc/rfc2440.txt

Software implementations of the OpenPGP standard are freely available for commercial use from the Free Software Foundation at http://www.gnupg.org.

Time Synchronization

Testing has shown that the clocks on all computer systems drift. It has also been surprising to see just how much they do. Time synchronization is required to assure that all trading partners transaction times are accurate. Time accuracy is dependent on how much a system's clock drifts, how frequently it is resynchronized and the accuracy of the source used for synchronization.

Authoritative time synchronization is now being provided by governmental agencies around the world based on a synchronized network of atomic clocks. In the United States this includes the U. S. Naval Observatory and the National Institute of Standards and Technology.

A easy way to obtain the current time is from the U. S. Naval Observatory's Web site at http://tycho.usno.navy.mil/cgi-bin/timer.pl. The output from this page can easily be edited and reformatted to set a local system's time. Commercial, shareware and public domain packages are also available to synchronize system times. Among them are NTP (which is an internet standard), internet daytime, nisttime / usnotime.

Further information on time synchronization may be found at the following Web sites:

http://www.eecis.udel.edu/~mills/ntp/test.html

http://tycho.usno.navy.mil/ntp.html

http://www.ccd.bnl.gov/xntp

http://www.txdirect.net/users/sfisher/clock.html

http://www.is.co.za/resources/ftpsite/tucows/softsync.html

APPENDIX B - Repudiation and Validation Examples

Repudiation and Validation examples:

When a transaction file is received using the EDM mechanism there are several questions that typically must be answered:

1.) Is the HTTP sender (from) valid to send to the HTTP 'to' party?
2.) Does the HTTP sender match the party who encrypted and signed the file?
3.) Does the HTTP sender match the sender within the file?
4.) Is that sender with the data valid to 'speak' for the parties transacting business?

Is the HTTP sender (from) valid to send to the HTTP 'to' party?

The first validation, determining that a party is a valid sender must be done during CGI execution. This is simply a 'look up' verification that the Common Code Identifier 'from' is recognized as a valid sender.

Does the HTTP sender match the party who encrypted and signed the file?

The next validation, determining that the HTTP sender is the same as the signer, requires that the following information be available:

The 'from' common code identifier (9 digit D-U-N-S® Number). This is the second field in the HTTP post message sent to the CGI. This information must be preserved from that earlier process and passed to the 'post-CGI' process.

The Pretty Good Privacy (PGP) or OpenPGP User ID associated with that same party

To compare these items a 'table' would most likely be established that would allow the post-CGI process to identify that there is a correlation between these identifiers. The origin of the 'from' identifier is the HTTP POST 'from' field. The origin of the PGP or OpenPGP user ID is the decryption process. The PGP or OpenPGP User ID of the signer is a byproduct of file decryption on a signed file. If PGP or OpenPGP software is executed from the command line the output would be presented in a format like:

Good signature from user "ABC CORP".
Signature made 1997/05/13 19:30 GMT
Plaintext filename: test3

If PGP or OpenPGP is executed using a program interface the User ID that signed the file will be provided in a buffer. Comparing this buffer to the expected User ID would serve to verify this value.

Does the HTTP sender match the sender within the file?

The data file itself indicates (in the case of X12 data) the sender and the intended recipient within the ISA segment. Although this may be the same (D-U-N-S® Number) as the 'from' data these fields are not standardized. This may require the use of a 'table' to relate these identifiers.

Consider also that, although it is strongly recommended that only a single ISA be contained within a file, that the process should account for the possibility of several ISA segments. This comparison will ensure that the parties used during translation are in fact the parties that sent, encrypted and signed the data.

Is that sender with the data valid to 'speak' for the parties transacting business?

This last validation is listed here only to complete the chain of identity. The process that would evaluate this relationship would typically be the business application. Since we have checked the identity through each step of this process this is the point at which the identity of the sender would finally be verified as having a business relationship to conduct the business specified.

APPENDIX C - Minimum Technical Characteristics and Guidelines for the Developer and User of the Customer Activities Web Site[1]

Browser Characteristics (includes defined NAESB WGQ current versions):

Features as supported by the latest Generally Available (GA) versions of both Netscape®[2] and Internet Explorer®[3] within 9 months of such GA version becoming available, including -

- Frames & Nested Frames
- Tables & Nested Tables
- HTML
- Cookies
- JavaScript
- SSL 128-bit RSA Encryption
- Style Sheets

Plug-ins (GA versions within 9 months of such GA versions becoming available)

- JAVA®
- ActiveX®[4] (Plug-in for Netscape®)
- Adobe Acrobat Reader® [5]
- Systems Incorporated
- Independent Computer Architecture (ICA®)[6] - Protocol used for remote control access to an application

Operating Systems:

Operating systems on a client workstation should be multithreaded and pre-emptive.

Hardware:

CPU	>=500 MHz
Memory	>=256 MB Physical
Display Resolution	>=1024 x 768, 16K colors
Connection	>=56 KB

---

1 Configuration shown indicates a minimum except where a specific level is established. 'Minimum' implies a level where a reasonable experience for the user may be achieved. These levels also indicate the level that a user may expect that a client has been tested. Results may be less than satisfactory, or may preclude use of a site, if the user chooses to use anything less than those levels shown.

2 Netscape® is a registered trademark of Netscape Communications Corp.

3 Internet® Explorer is a registered trademark of Microsoft Corporation.

4 ActiveX® is a registered trademark of Microsoft Corporation.

5 Adobe®, Acrobat®, and Reader® are registered trademarks of Adobe.

6 ICA® is a registered trademark of Citrix Systems Inc.

Example Configuration[1]

Hardware:	CPU: 500 MHz or higher Memory: 256MB Physical Display Resolution: 1024 x 768, 16K colors Pointing Device with left and right click capability
Operating Systems:	Windows®[2] 98 Windows® NT 4.0 Windows® 2000
Connection:	56KB 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®) Adobe Acrobat Reader® 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.

1 Specific products should be reviewed prior to implementation for Year 2000 compliance. Examples provided represent a non-comprehensive set of configurations that a client may use. This example list in no way should be construed as an endorsement by NAESB WGQ of any specific products. Other products meeting the minimum technical characteristics of the client workstation may be used.

2 Windows® is a registered trademark of Microsoft Corporation.

APPENDIX D - Minimum 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

	Minimum	Suggested
Connection Device:	33.3Kbs	Direct Connect
Operating System:	Multi-threaded & Preemptive	
RAM:	128 MB	>128 MB
Browser Capabilities:	Cookies & JavaScript Frames & Nested Frames Tables & Nested Tables HTML 3.2 Adobe Acrobat Reader®	
Display Resolution:	1024x768, 16k colors	>1024x768, 16k colors

Definitions:

Minimum 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]

	Minimum	Suggested
Hardware:	Pentium®[2] 200MHz or equivalent	Pentium® 500MHz or greater
RAM:	128 MB	> 128 MB
Communication Device:	33.3 Kbs	Direct Connect ISDN Satellite 56 KB modem DSL Cable-Modem
Monitor:	12" Laptop 15" Desktop	> 12" Laptop > 15" Desktop
Display Capabilities:	1024x768 16k colors	> 1024x768 > 16k colors
Operating System:	Windows® 95 System 8®[3] Solaris®[4] 2.6	Windows® XP Windows® 98 Windows® NT 4.0 Solaris® 8 System 9® Windows® 2000 Windows® ME Linux
Browser:	Microsoft Internet Explorer® Netscape® Communicator	Microsoft Internet Explorer® Netscape® Communicator

1 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 NAESB WGQ of any specific products. Other products supporting technical implementation may be used.

2 Pentium® is a registered trademark of Intel Corporation.

3 System 8® and System 9® are registered trademarks of Apple Computers, Inc.

4 Solaris® is a registered trademark of Sun Microsystems, Inc.

Informational Postings Web Site Developer Technical Characteristics

User's environment supporting the above minimum characteristics should be able to access all NAESB WGQ 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 except as specifically identified in this Appendix.

APPENDIX E - MINIMUM TECHNICAL CHARACTERISTICS FOR EDM COMMUNICATIONS

The following ports may be used by EDM developers and should be made available in user environments.

Allowable TCP Ports (not UDP ports)

HTTP HTTPS 80, 443, 5713, 6112, 6304, 6874, 7403
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. If and when NAESB WGQ 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 NAESB WGQ approved plug-ins and modules. Please refer to the NAESB WGQ defined Minimum Technical Characteristics for Accessing Customer Activities Web Sites for the listing of NAESB WGQ approved plug-ins and modules.

**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.

ICA® is a registered trademark of Citrix Systems Inc.

JAVA® is a registered trademark of Sun Microsystems, Inc.