TAB 4 – BUSINESS PROCESS AND PRACTICES

[Editor's Notes – to be deleted after review]

Section/ Paragraph	Area to Change/Comment	Suggested Change
[all]	"Transportation Service Provider" and "TSP"; these sound like natural gas terms. Regardless, I think it needs to be changed due to the ambiguity.	No action taken. What term will we use in REQ? Once we decide, we will need to go through the entire document and replace.
[all]	"Natural Gas" or "Gas"	"Energy"
[all]	"GISB" or "Gas Industry Standards Board"	"NAESB" or "NAESB REQ"
[all]	"3rd party"	"third-party"
[all]	"shippers"	"parties"
[all]	Name of REQ EDM? I used "EDM-REQ" to differentiate from NAESB WGQ EDM	Used EDM-REQ to differentiate REQ implementation from WGQ; can easily be globally replaced later.
[all]	General editing	Tightened up language using standard techniques (e.g. "utilize" becomes "use")
A	"Gas Industry"	"Electric Industry", even better "Energy Industry"
A, para 1	Language about EBB and FF does not apply	Delete language about EBB and FF
A, para 1	Need language regarding the reasons for an EDM for REQ; includes: need for future collaboration w/ WGQ; scope of initial EDM-REQ;	Added language "Role of EDM-REQ in NAESB
A, para 1	Need REQ-specific language for the role of the Internet EDM in REQ, including: large volumes, large transactions; existing implementations of EDM; ebXML; AS2; of EDI; of XML	Added language
A, para 1	XML: my understanding is that we need to address this in the standard.	Included some language; needs to be expanded and made consistent throughout document
A, para 2	Language about EBB and FF does not apply	Delete down to "separated flat files".
A, para 2	"Protect from non-repudiation" is worded incorrectly	Maybe "with non-repudiation"
A, para 3	Language about EBB	Delete entire paragraph
A, para 4	Questions in front can be removed; instead simply state value statement.	Deleted
A, para 28	"Pipeline"	Replaced with "Energy"
A, para 30	Need language about OpenPGP	Language added by Dick B
C, 4.1	Principles; deleted a bunch of them; should we renumber?	No action taken.
C, 4.1.1, 8, 11, 13, 16–35, 38	Language about EBB, IPs, and/or FF	Deleted relevant language or bullet
C, 4.2	Definitions; deleted a bunch, adding some: should we renumber?	No action taken
C, 4.2	Should we add a list of REQ entity types (LDC,	Added some then stopped. Are these

	TDSP, EDC, CR, ESP, ESCO, etc)	needed?
C, 4.2.1-10, 12-20	Language about EBB, IPs, and/or FF	Deleted relevant language or bullet
C, 4.2.21	Need language describing Failover scenario/process	Added language
C, 4.2.29	We reference 'trading partner agreement' and should have a definition. Will there be an REQ standard?	Added language re: trading partner agreement
C, 4.3	Standards: deleted a bunch; will be adding some; should we renumber	No action taken
C, 4.3.2	Language about 'pipeline'	Deleted language.
C, 4.3.3	Language about 15-minute window: does this apply to REQ and EDI/EDM?	No action taken
C, 4.3.4	Data retention requirements	Language modified by Dick B
C, 4.3.15	Need Open PGP language	Modified to include Open PGP language
C, 4.3.16	Appears to be related to IP or EBB mechanisms	Deleted
C, 4.3.5-7, 9, 17-35, 37-52, 54-63, 65-69, 72-73, 75-76, 78-86	Language about EBB, IPs, and/or FF	Deleted relevant language or bullet
C, 4.3.87	Language talks about changing business rules	Deleted
C, 4.3.88	Need 128-bit language	Added by Dick B
D, 7.3.24	Not relevant to REQ	Deleted
D, 7.3.35	Not relevant to REQ	Deleted

A. OVERVIEW

Role of Internet Electronic Transport (ET) in NAESB WGQ, REQ, and RGQ Quadrants

Business processes defined by NAESB quadrants require the exchange of transactions and transaction data. The Internet ET, in concert with Quadrant-specific Electronic Delivery Mechanisms (QEDMs), enables NAESB parties to securely and reliably exchange transactions over the Internet. Internet ET electronic 'packages' are created using the standards defined in this document.

~~—~~Version ??XX (OPEN ISSUE 028) of the Internet ET standard incorporates all technical specifications of the NAESB WGQ EDM Version 1.6, including m~~M~~utually-agreeable business practices to protect the sender of a document with non-repudiation and with digitally-signed Error Notifications.

Business Reasons for Using Internet ET

Using the Internet ET for communications standardizes how transactions and other electronic packages are exchanged among trading partners. ~~, a trading party needs to support fewer connections to its trading partners. T~~This ~~can~~ eliminates or reduces the complexity of different connection methods for different trading partners.

??security, error notifications/messages, minimum technology requirements, browser and batch capabilities; payload-agnostic; efficiency; open technologies; low-cost; PAIN;

Roles in Electronic Commerce

In most NAESB business processes, one party initiates, or sends, a transaction and the other party receives the transfer. The sender is referred to as the Client and the receiver is referred to as the Server. Parties ~~You should expect to~~ act in both the Client and Server roles during the electronic commerce process. Once a payload file is successfully received for processing, the original receiving party switches to the Client role to send an acknowledgement back to the original sender. ~~Your~~ Internet ET implementations need~~s~~ to implement both Client and Server features.

The standards adopted for Internet ET should be adhered to by the trading parties as minimum standards. A trading party may offer additional functions or features as options but should not require their use. Such additional features or functions are termed "mutually agreed to". If both trading partners agree on the inclusion, the additional feature requirements will be met. If either trading party does not agree to the inclusion of additional features, then the partners must allow for transmission and receipt of data using the minimum standards.

The Trading Partner Agreement is a key reference in electronic commerce. It includes "designated site" for each partner, values used for variable parameters, and optional features that will be used by the partners (OPEN ISSUE 008).

In-house Development, COTS Software, and Outsourced Solutions

The NAESB Internet ET can be constructed and deployed with in-house development and resources, with consulting/development help from a third-party, with Commercial Off-The-Shelf (COTS) software or as an outsourced solution with a third-party. The best solution for each organization must be determined based on the assessment of specific needs and the resources available to that organization.

All parties should fully investigate the ramifications of implementing electronic commerce using the Internet. This includes ensuring that all customer data, internal data, and applications are secured from intruders or other

parties not authorized for access.

Participation in electronic commerce over the Internet involves hardware, software, and technical expertise. Hardware requirements may include a server to receive incoming Internet ET packages and a firewall to block intruder access. Software includes operating software for the servers, including the firewall, programming languages which support Internet technologies, and encryption/decryption software to provide security during the transfer. Technical expertise may be involved in the development and maintenance of server applications to process incoming files as well as applications to initiate communication with the server of your trading partner.

Third-party providers offer a variety of services from a full "turn key" solution to assistance where you require it, including programming, system configuration, system administration and private communication links.

Internet ET Network Connections

Trading partners should maintain redundant connections to the public Internet for Internet ET sites. These redundant connections should be topographically diverse paths to minimize the probability of a single point of failure. Three possible approaches to redundant connections are:

1. Maintain multiple ISPs and multiple points of connectivity, each of which was identified by the same URL making the process of redundancy transparent to the sender.
2. Maintain different Internet connectivity URLs (presumably on topographically different ISPs). For this to result in communication redundancy, the sender should know of the existence of the secondary URL and have programming in place that will automatically switch batch-browser transmissions to the secondary URL when the primary URL is unavailable.
3. Maintain multiple connections to the same ISP. This involves only one URL but the presumption would be that the ISP would provide alternate diverse paths for the URL.

Servers may maintain multiple URLs and, if such have been disclosed, the sender should attempt to use these during primary URL outages. The redundant public Internet connections can be through a single ISP or multiple ISPs. If multiple URLs are provided for Internet ET access, the following conditions should be met:

- The information provided by each URL should be exactly the same, although the "trans-id" sequences may differ.
- The trading partners should be informed of both URLs and their availability by system wide notice or by TPA.
- The URLs should be identified as primary and secondary if either:
  - There is a TSP connection speed difference between the URLs (The faster connection listed as primary)

    OR

    One URL is only available when the other is down (primary URL being the most available)
- The URLs should be listed as primary and alternate if:
  - The URLs have the same TSP connection speed

    AND

  - The URLs are customarily available simultaneously

A URL is considered available, in the context of communication redundancy, if all the IP facilities are properly functioning up to and including the HTTP service. This includes firewalls, DNS servers, routers, hubs, LANs, etc. between your HTTP server and your Internet Service Provider's point of presence.

In this context redundancy refers to normal operations redundancy, as opposed to disaster recovery contingencies.

Private network connections to access NAESB Internet ET sites may be at any point on a party's firewall boundary at the party's discretion on a non-discriminatory basis. The specific type and speed of their connection should be mutually agreed. It is at the discretion of the party how multiple private network connections should be managed.

Disaster recovery contingencies are not addressed in NAESB Internet ET.

TCP Communications

NAESB WGQ Principle 4.1.37 and NAESB WGQ Standard 4.3.70 restrict the TCP ports used as a standard for Internet ET communications. The use of NAESB standard TCP ports may require modifications in the client-side firewall to allow for communications with the various service providers' Internet ET implementations. Upon request, parties should indicate to their trading partners which specific TCP ports they require opened to conduct electronic communication. See Appendix E for a list of allowable TCP ports. (OPEN ISSUE 007)

??TCP guidelines will be reviewed, updated, and changes presented to the NAESB Executive Committees for adoption for inclusion in the next Internet ET release.

Major Functions of NAESB Internet ET

Communication Protocols

HTTP POST is the standard method for transporting Internet ET packages to trading partners. Internet ET packages are created using the "multi-part" content type.

Sending Transactions (Client)

A batch browser allows organizations to maximize their level of automation. The batch browser can be an event-driven mechanism used to push Internet ET packages to your trading partners in real-time or near -real-time, while providing better ~~logging and~~ audit trails.

Receipt of Transactions (Server)

Receipt of Internet ET packages and transaction payloads require a Receiving program. The Receiving program:

- Parses the Internet ET package parameters and files to determine if the appropriate parameters were transmitted
- Saves a log including a time stamp for the package
- Stores the payload file
- Sends the Receipt as an HTTP Response to the Client with the timestamp and other required Receipt elements

??In some cases the Receiving program decrypts the file prior to sending the Receipt. In this scenario decryption errors would be communicated in the Receipt. Some trading partners decrypt after sending the Receipt. Decryption errors, detected after the Receipt is sent, are communicated to trading partners using Internet ET Error Notification standards. Parties should notify trading partners of how decryption errors will be communicated.

If trading partners mutually agree to use signed Receipts, then the application would additionally attach a digital signature to the Receipt.

After the Receiving program performs its functions without errors, the payload file is forwarded to other processes including security, translation, and back-office systems.

Security

NAESB Internet ET establishes several security measures as standards to ensure a minimum level of confidence in conducting business over the Internet, and to provide uniformity in the implementation of security. Four security concepts, known as PAIN, are vital to protecting Internet ET packages :

- Data **P**rivacy
- **A**uthentication
- Data **I**ntegrity
- **N**on-repudiation

Data Privacy and Encryption

Privacy is the assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended. Data privacy is accomplished by encrypting payload files. Internet ET allows encryption using:

- PGP 6.5 or higher, with RSA keys. Previous versions of PGP are not compatible with OpenPGP.
  OR
- OpenPGP, defined by IETF RFC 2440. OpenPGP can be used on a mutually-agreed basis.

Starting in WGQ EDM v1.6 and Internet ET v1.0??, SSL is used to protect username and passwords.

Authentication

Authentication is the assurance to one entity that another entity is he/she/it claims to be. Basic authentication is the required standard to prevent intruders from connecting to Internet ET Web sites. Starting in NAESB WGQ EDM v1.6 and Internet ET v1.0??, SSL is used to protect username and passwords. Additional techniques such as firewall security enable further authentication.

Integrity

Integrity is the assurance to an entity that data has not been altered, intentionally or unintentionally, between there and here, or between then and now. ??Data Integrity is established via PGP/OpenPGP encryption, and via the “content-length” HTTP header field.

Non-Repudiation

Non-repudiation is the assurance to an entity that a party cannot deny having engaged in the transaction, or having sent the electronic message. It is like a Notary seal. The Sender of a file includes in the Internet ET package a digital signature that is created using their Private key. The Receiver knows the Sender is legitimate by decoding the digital signature using the Sender’s Public key.

B. GENERAL STANDARDS

Principles:

0.1.1 An entity is a person or organization with sufficient legal standing to enter into a contract or arrangement with another such person or organization (as such legal standing may be determined by those parties) for the purpose of conducting and/or coordinating ~~natural gas~~ energy transactions.

0.1.2 ~~For NAESB WGQ purposes, t~~There should be a unique entity common code for each entity name and there should be a unique entity name for each entity common code.

Standard:

0.3.1 Entity common codes should be "legal entities", that is, Ultimate Location, Headquarters Location, and/or Single Location (in Dun & Bradstreet Corporation ("D&B") terms). However, in the following situations, a Branch Location (in D&B terms) can also be an entity common code.

1. when contracting party provides a D-U-N-S®**1** Number at the Branch Location level; or
2. to accommodate accounting for an entity that is identified at the Branch Location level.

(OPEN ISSUE 001)

1 D-U-N-S® is a registered trademark of Dun & Bradstreet, Inc.

C. ELECTRONIC DELIVERY MECHANISM RELATED STANDARDS

Principles:

4.1.1 [Deleted]

4.1.2 The Internet Electronic Transport (ET) ~~Electronic Delivery Mechanism~~ does not pick winners, rather it should create an environment where the marketplace can dictate a winner or winners.

4.1.3 The solutions should be cost effective, simple and economical.

4.1.4 The solutions should provide for a seamless marketplace for energy.

4.1.5 [Deleted]

4.1.6 Parties ~~Data providers (transportation service providers)~~ should interface with third-party vendors according to NAESB Internet ET standards.

4.1.7 Electronic communications between parties to the transaction should be done on a non-discriminatory basis, whether through an agent or directly with any party to the transaction.

4.1.8 [Deleted]

4.1.9 ~~Service providers should post clear and precise business processing rules at the designated site, or in writing, upon request.~~

4.1.10 ~~There should be at least one standard (computer-to-computer exchange of transactional data) for data exchange format.~~

4.1.11 [Deleted]

4.1.12 Protocols and tools that parties elect to support should be “Internet-compatible”.

4.1.13 ~~Regarding the request that EBBs need to provide the ability to create and print specialized reports, the data should be made available so as to permit the users of the information to download the data to be used in their applications~~.

4.1.14 The industry should use standard policies and guidelines for testing. ~~These guidelines are contained in the REQ EDM specification. new data sets. These guidelines are currently being developed using the NAESB WGQ guideline adoption procedures (GAP) (GISB Version 1.0).~~

4.1.15 The NAESB Internet ET should not set standards for site-level security. Individual organization security standards should be relied upon.

4.1.16 [Not applicable to ET]

4.1.17 [Not applicable to ET]

4.1.18 [Not applicable to ET]

4.1.19 [Not applicable to ET]

4.1.20 [Not applicable to ET]

4.1.21 [Not applicable to ET]

4.1.22 [Not applicable to ET]

4.1.23 [Not applicable to ET]

4.1.24 [Not applicable to ET]

4.1.25 [Not applicable to ET]

4.1.26 [Not applicable to ET]

4.1.27 [Not applicable to ET]

4.1.28 [Not applicable to ET]

4.1.29 [Not applicable to ET]

4.1.30 [Not applicable to ET]

4.1.31 [Not applicable to ET]

4.1.32 [Not applicable to ET]

4.1.33 [Not applicable to ET]
4.1.34 [Not applicable to ET]
4.1.35 [Not applicable to ET]

4.1.36 Trading partners should maintain redundant connections to the public Internet for NAESB Internet ET Web sites. These redundant connections should be topographically diverse (duality of) paths to minimize the probability of a single point of failure.

4.1.37 Internet ET implementations should minimize the number of outbound ports required to be opened on the client-side firewall.

4.1.38 [Not applicable to ET]

4.1.39 Trading Partners should mutually select and use a version of the NAESB Internet ET standards under which to operate, unless specified otherwise by government agencies. Trading Partners should also mutually agree to adopt later versions of the NAESB Internet ET standards, as needed, unless specified otherwise by government agencies.

Definitions

4.2.1 [Not applicable to ET]

4.2.2 [Not applicable to ET]

4.2.3 [Not applicable to ET]

4.2.4 [Not applicable to ET]

4.2.5 [Not applicable to ET]

4.2.6 [Not applicable to ET]

4.2.7 [Not applicable to ET]

4.2.8 [Not applicable to ET]
4.2.9 [Not applicable to ET]
4.2.10 [Not applicable to ET]

4.2.11 [Not applicable to ET]

4.2.12 [Not applicable to ET]

4.2.XX [Not applicable to ET]

4.2.13 [Not applicable to ET]

4.2.14 [Not applicable to ET]

4.2.15 [Not applicable to ET]

4.2.16 [Not applicable to ET]

4.2.17 [Not applicable to ET]

4.2.18 [Not applicable to ET]

4.2.19 [Not applicable to ET]

4.2.20 ??Testing electronic packages between trading partners includes testing of:
1. Connectivity;
2. Encryption/Decryption;
3. Digital signatures where appropriate

4.2.x21 "Failover" defines a scenario a prescribed process is executed when a NAESB Internet ET Client fails to establish a connection to the target NAESB Internet ET Server.

4.2.x22 "Trading Partner" is a party that enters into an agreement with another party to transact business electronically using the Internet ET standard.

4.2.x23 "Originating party" is any party originating/creating the package . This could also include a third-party.

4.2.x24 "Third-Party" is any organization that a trading party uses to provide services to comply with the required elements of the Internet ET.

4.2.x25 "Receiving Party" is any party that hosts (either in-house or outsourced) an Internet ET compliant server capable of receiving Internet ET packages.

4.2.x26 "Trading Partner Agreement" is a legal agreement between trading parties. This agreement often dictates service level agreements and problem remediation processes. (OPEN ISSUES 008)

Standards

4.3.x1 All parties sending and receiving data should accept a TCP/IP connection.

4.3.x2 ??On time stamping, data leaves control of the originator by the same time (deadline), regardless of mechanism (3rd party service provider time stamp is acceptable) and 15 minutes of communication time should be available to allow accumulation of all transactions to the pipeline. A standard network protocol (TCP/IP) should be in service for direct connect to the pipeline designated site by 4/1/97.

4.3.x3 ??Originating party is any system originating/creating the document reflecting the transaction to be submitted (this could also include a third-party service provider or a transportation service provider's EBB). Within the 15-minute window the transaction should be received by the receiving party. Errors in transmission shall be governed by the terms and conditions of the trading partner agreement between the parties. The receiving party may also waive the 15-minute window requirement at its own discretion. ~~[Deleted]~~[Not applicable to ET]

4.3.4 Trading partners should retain audit trail data for at least 24 months. This data retention requirement does not otherwise modify statutory, regulatory, or contractual record retention requirements. (OPEN ISSUE 033)

4.3.5 [Not applicable to ET]

4.3.6 [Not applicable to ET]

4.3.7 At a minimum, the designated site should be accessible via the public Internet. This specifically does not preclude location of the designated site on a private intranet as long as the designated site is accessible via the public Internet.

4.3.8 The minimum acceptable protocol should be HTTP. All sending and receiving parties should be capable of sending and receiving the HTTP versions supported by NAESB Internet ET.

4.3.9 There is a time stamp ("time-c"~~HTTP Timestamp~~) that designates the time that a file is received at the designated site. The receiving party should generate a timestamp upon the successful receipt of a complete file and send an immediate response to the sending party. The timestamp should be generated by the Receiving program of the receiving party, prior to further processing by the Receiving program.

4.3.10 The timestamp should be included in the HTTP Response back to the sender of the original HTTP package~~transaction~~. The server clock generating the timestamp should be synchronized with the National Institute of Standards and Technology (NIST) time in order to mitigate discrepancies between the clocks of the sender and receiver. (OPEN ISSUE 010)

4.3.11 The HTTP Response should be sent to the sending Internet Protocol (IP) address. Other response documents should be returned to the official designated site defined in the Trading Partner Agreement (OPEN ISSUE 008).

4.3.12 As a minimum, within a trading partner agreement, one designated site for receipt should be identified for each trading partner. That site should be identified by a specific Uniform Resource Locator, (URL). This does not preclude multiple designated sites being mutually agreed to between trading partners. (OPEN ISSUE 008)

4.3.13 The sender should make three attempts to complete a unit of work. A unit of work consists of one complete HTTP POST transaction as defined in the technical specification of the HTTP protocol (Internet Engineering Task Force RFC 1945). The roles of sender and receiver are also defined in that document. After three failed attempts, it should be considered a failure. ??timeframe between failures

4.3.14 The roles of sender and receiver are defined in the following table. The entire table defines a unit of work:

Client (Sender)	Server (Receiver)	Receiving Program (Receiver)
	Listen for Connect	
Connect	Accept Connection	
Write	Read	Start of Receipt
Write	Read	
EOF (send)	Read	End of Receipt
Read (HTTP response)	Write (HTTP response)	
Received		
EOF (HTTP response)		

4.3.15 Trading partners should implement all security features (privacy, secure authentication, integrity, ~~privacy,~~ and non-repudiation) using a file-based approach via a commercially available implementation of PGP 6.5 or greater (or compatible with PGP 6.5) or, on a mutually agreed basis, an OpenPGP compatible product. Trading partners should also implement basic authentication. These technologies support 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. Encryption keys should have a limited lifetime whose duration is determined by the key's owner. A key's end of life is expressed in the expiration date field contained in each public key. A lifetime of one year or less is recommended.

4.3.16 [Not applicable to ET]
4.3.17 [Not applicable to ET]
4.3.18 [Not applicable to ET]
4.3.19 [Not applicable to ET]
4.3.20 [Not applicable to ET]
4.3.21 [Not applicable to ET]

4.3.22 [Not applicable to ET]
4.3.23 [Not applicable to ET]
4.3.24 [Not applicable to ET]

4.3.25 [Not applicable to ET]
4.3.26 [Not applicable to ET]
4.3.27 [Not applicable to ET]

4.3.28 [Not applicable to ET]

4.3.30 [Not applicable to ET]
4.3.31 [Not applicable to ET]

~~A unit of work consists of one complete HTTP transaction as defined in the technical specification of the HTTP protocol (Internet Engineering Task Force RFC 1945). The roles of sender and receiver are also defined in that document.~~

4.3.32 [Not applicable to ET]

4.3.33 [Not applicable to ET]

4.3.34 [Not applicable to ET]

4.3.35 [Not applicable to ET]

4.3.36 Internet protocols should be used for accessing all industry business functions.
[Get rid of 38 through 55]

4.3.37 Web browser interface should use Internet compatible common browser software.

4.3.38 [Not applicable to ET]

4.3.39 [Not applicable to ET]

4.3.40 [Not applicable to ET]

4.3.41 [Not applicable to ET]

4.3.42 [Not applicable to ET]

4.3.43 [Not applicable to ET]

4.3.44 [Not applicable to ET]

4.3.45 [Not applicable to ET]

4.3.46 [Not applicable to ET]

4.3.47 [Not applicable to ET]

4.3.48 [Not applicable to ET]

4.3.49 [Not applicable to ET]

4.3.50 [Not applicable to ET]

4.3.51 [Not applicable to ET]

4.3.52 [Not applicable to ET]

4.3.53 [Not applicable to ET]
4.3.54 [Not applicable to ET]

4.3.55 [Not applicable to ET]

4.3.x56 The industry should use common codes for ~~location points and~~ legal entities when using Internet ET. ~~communicating via EDI/EDM, EBB/EDM and/or XML~~FF/EDM.

4.3.57 [Not applicable to ET]

4.3.58 [Not applicable to ET]

4.3.59 [Not applicable to ET]

4.3.60 [Not applicable to ET]

4.3.61 [Not applicable to ET]

4.3.62 [Not applicable to ET]

4.3.63 [Not applicable to ET]

4.3.64 Private network connections to NAESB Internet ET ~~REQ EDM~~ Web sites, which include all NAESB ~~WGQ REQ~~ Internet ET standardized Internet communication, may be at any point on a party's firewall boundary at the party's discretion on a non-discriminatory access basis. The specific type and speed of these connections should be mutually agreed. It is at the discretion of each party on how multiple private network connections should be managed, so long as such management is done on a non-discriminatory access basis.

4.3.65 [Not applicable to ET]

4.3.66 [Not applicable to ET]

4.3.67 [Not applicable to ET]

4.3.68 [Not applicable to ET]

4.3.69 [Not applicable to ET]

4.3.70 Parties should be limited to the NAESB Internet ET approved list of available TCP ports and UDP ports for Internet ET ~~EDM~~ implementations included in Appendix E?? of the Internet ET ~~Electronic Delivery Mechanism Related~~ Standards Manual. (OPEN ISSUE 009)

4.3.71 Internet ET implementations should not require any inbound ports to be opened on the client-side firewall.

4.3.72 [Not applicable to ET]

4.3.73 [Not applicable to ET]

4.3.74 [Not applicable to ET]

4.3.75 [Not applicable to ET]

4.3.76 [Not applicable to ET]

4.3.77 [Deleted]

4.3.78 [Not Applicable to ET]

4.3.79 [Not Applicable to ET]

4.3.80 [Not Applicable to ET]

4.3.81 [Not Applicable to ET]

4.3.82 [Not Applicable to ET]

4.3.83 [Not Applicable to ET]

4.3.84 [Not Applicable to ET]

4.3.85 [Not Applicable to ET]

4.3.86 [Not Applicable to ET]

4.3.87 [Not Applicable to ET]

4.3.88 For Internet ET, ~~EDM,~~ 128-bit Secure Socket Layer (SSL) encryption should be used.

D. INTERPRETATIONS

NAESB ~~WGQ~~ REQ has adopted the following interpretations of standards that relate to Electronic Delivery Mechanism Related Standards implementation:

[NONE TO DATE]

7.3.24 [Not applicable to ET]

7.3.35 [Not applicable to ET]