



North American Energy Standards Board

1301 Fannin, Suite 2350, Houston, Texas 77002
Phone: (713) 356-0060, Fax: (713) 356-0067, E-mail: naesb@naesb.org
Home Page: www.naesb.org

COPYRIGHT NOTICE

The following North American Energy Standards Board (NAESB) final action or published standards is protected by federal copyright and a limited waiver has been granted for your access for **evaluation purposes only**. It should not be distributed or shared in any manner other than to task force members of the Illinois Commerce Commission for their review and evaluation. If you are not a member of NAESB and would like to use the following final action or published standards for purposes other than evaluation, please contact the NAESB office at 713-356-0060 or naesb@naesb.org for permission or purchase.



**North American Energy Standards Board
Retail Gas Quadrant
Retail Electric Quadrant**

Business Practice Standards

Model Business Practices and Models Relating To

**Master List of Defined Terms
Market Participant Interactions
Creditworthiness
Billing and Payments
Quadrant-Specific Electronic Delivery Mechanism
Distribution Company – Supplier Disputes
Contracts
Internet Electronic Transport**

September 27, 2005

Minor Corrections Applied July 14, 2006 and January 29, 2008

Copyright © 2005 North American Energy Standards Board, Inc.
All rights reserved.

The North American Energy Standards Board (“NAESB”) disclaims and excludes, and any user of the NAESB standard acknowledges and agrees to NAESB’s disclaimer of, any and all warranties, conditions or representations, express or implied, oral or written, with respect to the standard or any part thereof, including any and all implied warranties or conditions of title, non-infringement, merchantability, or fitness or suitability for any particular purpose (whether or not NAESB knows, has reason to know, has been advised, or is otherwise in fact aware of any such purpose), whether alleged to arise by law, by reason of custom or usage in the trade, or by course of dealing. Each user of the standard also agrees that under no circumstances will NAESB be liable for any special, indirect, incidental, exemplary, punitive or consequential damages arising out of any use of, or errors or omissions in, the standard.

The NAESB Retail Gas Quadrant (“RGQ”) and Retail Electric Quadrant (“REQ”) Model Business Practices related to defined terms, market participant interactions, creditworthiness, billing and payments, quadrant-specific electronic delivery mechanisms, distribution company – supplier disputes, contracts, and internet electronic transport, and any amendments or errata thereto, are protected by NAESB’s federal copyright 2005. NAESB hereby grants the authorized users who are NAESB members in good standing permission to reproduce material therein for internal reference and use and not for use by any unauthorized third parties. Reproduction in any other form, or for any other purpose, is forbidden without express permission of NAESB. Copies are available for purchase from NAESB. This non-exclusive limited license is non-transferable and may be revoked without notice upon violation of the terms contained herein or any applicable law or regulation. Each user grants NAESB the right to audit its use to assure compliance with these terms.

The model business practices follow a numbering convention which is q.x.y.z.a, where:

- q RXQ – Applicable to both REQ and RGQ
 REQ – Applicable only to REQ
 RGQ – Applicable only to RGQ

- x 0 – Defined Terms
 1 – Market Participant Interactions MBPs
 2 – Creditworthiness MBPs
 3 – Billing and Payments MBPs
 4 – Distribution Company – Supplier Disputes MBPs
 5 – Quadrant-Specific Electronic Delivery Mechanism MBPs
 6 – Contracts
 7 – Internet Electronic Transport MBPs

- y 1 – Principles
 2 – Definitions
 3 - Model Business Practices
 4 – Models

- z Functional Grouping

- a Sequentially assigned number

Terms used:

- MBP - Model Business Practice
- NAESB - North American Energy Standards Board
- RGQ - Retail Gas Quadrant
- REQ - Retail Electric Quadrant

Table of Contents:

Master List of Defined Terms	Page 4
Market Participant Interactions MBPs	Page 9
Creditworthiness MBPs	Page 20
Billing and Payments MBPs	Page 39
Distribution Company – Supplier Disputes MBPs	Page 56
Quadrant-Specific Electronic Delivery Mechanism MBPs	Page 62
Contracts Related MBPs	Page 123
Internet Electronic Transport MBPs	Page 153
Version Notes	Page 213
Appendix 1	Page 214

MASTER LIST OF DEFINED TERMS

- RXQ.0.2.1 Applicable Regulatory Authority:** The state regulatory agency or other local governing body that provides oversight, policy guidance, and direction to any parties involved in the process of providing energy to retail access Customers through regulations and orders.
- RXQ.0.2.2 Applicant:** The party seeking credit from another party.
- RXQ.0.2.3 Assumption of Receivables:** The payment processing method in which the Billing Party assumes the Non-Billing Party's receivables and sends the Non-Billing Party payment at predetermined intervals for all Non-Billing Party amounts that are billed, payable to the Non-Billing Party, and do not have a status of In Dispute, in accordance with the tariff, Billing Services Agreement or other Governing Document regardless of when (or whether) the Customer pays the Billing Party.
- RXQ.0.2.43 Batch Flat-file:** The automated computer-to-computer transfer of Flat-files.
- RXQ.0.2.4 Bill Ready:** A Consolidated Billing practice in which the Billing Party receives the calculated charge amount(s) directly from the Non-Billing Party in lieu of the Billing Party calculating it directly from the rate.
- RXQ.0.2.5 Billing Party:** The party performing billing services for one or more parties.
- RXQ.0.2.6 Billing Services Agreement:** A legally binding document between the Distribution Company and the Supplier used when one of the parties is performing Consolidated Billing for the other party. Such document sets forth the expectations and responsibilities of each party.
- RXQ.0.2.7 Business Day:** As defined in the Governing Documents.
- RXQ.0.2.44 Business Rule Change:** Any a) change in the presence and/or the acceptable content of a data element sent by the changing party; b) new business response to an accepted data element received by the changing party; c) new business response to the acceptable content of a data element received by the changing party; or d) new intended business result.
- RXQ.0.2.8 Cash Deposit:** Money provided by one party to the other to secure performance of an agreement or compensate for possible loss or damage.
- RXQ.0.2.9 Certificate of Authority:** A document attesting to the name(s) and signature(s) of the officer(s) authorized to execute a particular instrument.

RXQ.0.2.10 Challenge: The Applicant's request for a review of the Creditor's creditworthiness determination made shortly after that determination.

RXQ.0.2.11 Confidential Information: Nonpublic information concerning the financial condition of the Applicant, or any of the Applicant's affiliates, that is disclosed to the Creditor by or on behalf of the Applicant or Applicant's affiliates.

RXQ.0.2.12 Consolidated Billing: The billing option in which the Distribution Company or Supplier renders a Customer bill consolidating the energy, transmission / transportation and distribution charges of the Distribution Company and the Supplier, for which a single payment from the Customer is expected.

RXQ.0.2.13 Credit Application Form: The Creditor's form for obtaining identification and financial data about an Applicant.

RXQ.0.2.14 Creditor: The party granting credit to another party.

RXQ.0.2.15 Cure Period: A period of time specified in a contract allowing a defaulting party to rectify the default, during which time the Creditor would not be allowed to exercise its remedies.

RXQ.0.2.16 Customer: Any entity that takes gas and/or electric service for its own consumption.

RXQ.0.2.45 D-U-N-S® Number: The D-U-N-S® Number is a 9-digit number assigned to companies by the Dun & Bradstreet Corporation .The D-U-N-S+4® Number is a 10- to 13-digit number, where characters 10 through 13 are arbitrarily assigned by the owner of the D-U-N-S® Number.

RXQ.0.2.17 Distribution Company: A regulated entity which provides distribution services and may provide energy and/or transmission/transportation services in a given area.

RXQ.0.2.18 Distribution Company Operational Manuals: Documents prepared and published by Distribution Companies that describe, in detail the operating processes/procedures used to perform retail access functions.

RXQ.0.2.19 Distribution Company-Supplier Service Agreement: A bi-lateral contractual agreement between the Distribution Company and the Supplier that determines the parties' roles, responsibilities, and interactions in serving retail access Customers. Usually this will be the master agreement that will cover most aspects of providing retail access service. There may be one or more subsidiary agreements, covering specific functional areas.

- RXQ.0.2.20 Dual Billing:** The billing option in which the Distribution Company and Supplier render separate Customer bills for the products and services each provides.
- RXQ.0.2.46 EDI/EDM:** Electronic Data Interchange/Electronic Delivery Mechanism. Describes ANSI ASC X.12 computer-to-computer electronic data interchange of information in files as mapped from RXQ.x.4.z model business practices in the NAESB RXQ Implementation Guides and communicated between Trading Partners over the Internet using the NAESB Internet Electronic Transport (ET).
- RXQ.0.2.47 Entity:** 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 energy transactions.
- RXQ.0.2.48 Entity Common Code:** The D-U-N-S® or D-U-N-S+4® number used as the common company identifier. Entity common codes should be 'legal entities,' that is, Ultimate Location, Headquarters Location, and/or Single Location in Dun & Bradstreet terms.
- RXQ.0.2.21 Event-driven Reconsideration:** A re-evaluation of an Applicant's creditworthiness performed in response to a Material Change in its credit rating or financial condition
- RXQ.0.2.49 FF/EDM:** Flat File/Electronic Delivery Mechanism. describes a standardized Flat-file electronic data interchange of information in files as mapped from the RXQ.x.4.z model business practices.
- RXQ.0.2.50 Flat-file:** An ASCII comma-separated-value (CSV) file with the characteristics as defined in the RXQEDM model business practices.
- RXQ.0.2.22 Governing Documents:** Documents that determine the interactions among parties, including, but not limited to, regulatory documents (e.g., tariffs, rules, regulations), contractual agreements, and Distribution Company Operational Manuals.
- RXQ.0.2.23 Guarantor:** The issuer of a Guaranty.
- RXQ.0.2.24 Guaranty:** An obligation to pay the unpaid obligations of a third party Applicant to Creditor upon certain conditions being met.
- RXQ.0.2.25 In Dispute:** A bill status that prevents collection action from being taken on the disputed amount.
- RXQ.0.2.51 Interactive Flat-file:** Describes the FF/EDM transfer of Flat-files using an interactive browser.
- RXQ.0.2.26 Letter of Credit:** A letter issued by a bank authorizing the beneficiary to draw up to a stated amount of money from the issuing bank, its branches, or other associated banks or agencies, provided that the drawing conditions of the letter are met.

- RXQ.0.2.27 Market Participant:** A party engaged in the process of providing competitive retail energy to end-use customers including, but not limited to, the Distribution Company, the Supplier, the Registration Agent, the settlement agent, and the meter reading entity.
- RXQ.0.2.28 Market Participant Service Agreements:** All contractual agreements between or among Market Participants that determine the parties' roles, responsibilities, and interactions in serving retail access Customers. These include the Distribution Company-Supplier Service Agreement and any other agreements executed by Market Participants to facilitate retail access (e.g. a contract between a meter reading entity, the Distribution Company, and the Supplier detailing how usage data will be provided).
- RXQ.0.2.29 Material Change:** Any change in the Applicant's (or Guarantor's) financial or other condition that might reasonably affect the amount of credit extended to that Applicant or may impact the Applicant's ability to perform on its obligations.
- RXQ.0.2.30 Non-Billing Party:** The party whose charges are being combined into a statement (or invoice) prepared and rendered by another party.
- RXQ.0.2.31 Pay As You Get Paid:** The payment processing method in which the Billing Party forwards payment to the Non-Billing Party for the Non-Billing Party charges only after receiving payment.
- RXQ.0.2.32 Prepayment:** Money provided by one party to the other to pay for goods or services not yet rendered.
- RXQ.0.2.33 Rate Code:** A product identifier used in a billing system which contains all information, such as description and price, needed to bill for that product. One or more Rate Codes may be billed on a single account.
- RXQ.0.2.34 Rate Ready:** Refers to the practice in which the Non-Billing Party provides rate information to the Billing Party sufficient to calculate the Non-Billing Party's charges.
- RXQ.0.2.35 Registration Agent:** An entity facilitating switches and performing record-keeping for a specified geographical area.
- RXQ.0.2.52 RXQEDM:** Electronic Delivery Mechanism model business practices for the NAESB RGQ and REQ quadrants that govern package payload file contents, including ANSI ASC X.12 EDI, Flat-file and other formats.
- RXQ.0.2.36 Security Interest in Collateral:** A right, title, claim, or share in assets that exists by contract as security for payment or performance of an obligation that is acceptable to the creditor.

- RXQ.0.2.37 Service Delivery Point:** A physical metered and/or unmetered service location supplying energy to a Customer premise.
- RXQ.0.2.38 Single Retail Supplier Billing:** The billing option in which the Supplier renders a Customer bill for all energy, transmission/transportation, and distribution related charges. The Supplier purchases or otherwise acquires energy, transmission/transportation and distribution services, and therefore all charges on the bill are Supplier charges. A single payment from the Customer is expected.
- RXQ.0.2.39 Supplier:** Persons engaged in the competitive sale of energy to end-users.
- RXQ.0.2.40 Surety Bond:** An obligation of a third party that covers payments to the Creditor in the event that the Applicant fails to meet its obligations.
- RXQ.0.2.41 Switch Request:** A request from a Supplier to switch a Customer to begin receiving service from that Supplier.
- RXQ.0.2.53 Testing:** Verification that Trading Partners have the system capabilities in place for: a) intended business results, b) proposed electronic transport, including security, enveloping, cryptography; and c) Electronic Delivery Mechanisms (EDI/EDM or FF/EDM), including data validity, model business practice compliance, etc.
- RXQ.0.2.54 Trading Partner:** A party that enters into an agreement with another party to transact business electronically using NAESB model business practices.
- RXQ.0.2.43 Trading Partner Agreement:** A legally binding agreement between any two Market Participants defining each party's expectations and responsibilities for doing business with each other using Uniform Electronic Transactions.
- RXQ.0.2.55 Translator:** A program or set of programs that process the contents of payloads, applying ANSI ASC X.12 and other model business practices, and transform the information to other formats.
- RXQ.0.2.42 Uniform Electronic Transaction:** Standard data arrangements for trading information, making business requests and exchanging other information, encompassing a number of electronic media and utilizing specified transport protocols.

MARKET PARTICIPANT INTERACTIONS

Executive Summary

The procedures and processes described in these Market Participant Interactions Model Business Practices are intended to provide a consistent framework for identifying and documenting the roles of the various Market Participants involved in serving Customers' energy needs in competitive markets. Use of these practices should ensure Customers participating in competitive electric and natural gas markets are served in a consistent and efficient manner.

Expectations, obligations and performance standards for Market Participants are typically defined by the Governing Documents. Although the specifics of the documents will vary depending on the jurisdiction, following the guidelines proposed in these practices should ensure that key elements are in place so that all parties are aware of their responsibilities.

These model business practices identify the areas of Market Participant Interactions that are typically addressed within the various types of Governing Documents, such as:

- Regulatory documents,
- Contractual agreements, and
- Distribution Company operation manuals.

These model business practices will guide the interactions among Market Participants including:

- Suppliers in their interactions with Distribution Companies
- Distribution Companies in their interactions with Suppliers
- Other Market Participants in their interactions with Suppliers, Distribution Companies, or both. These interactions include, but are not limited to:
 - Performing the Registration Agent function (when not performed by the Distribution Company),
 - Performing meter reading,
 - Performing billing,
 - Aggregating (but not serving) Customer loads, or
 - Performing/supporting settlement.

In addition, these model business practices provide guidance concerning the Distribution Company certification of a Supplier's, or other Market Participant's, ability to perform the role required of them within the Distribution Company's service territory.

Introduction

The North American Energy Standards Board (“NAESB”) is a voluntary non-profit organization comprised of members from all aspects of the natural gas and electric industries. Within NAESB, the Retail Electric Quadrant (“REQ”) and the Retail Gas Quadrant (“RGQ”) focus on issues impacting the retail sale of energy to end-use Customers. REQ / RGQ Model Business Practices are intended to provide guidance to Distribution Companies, Suppliers, and other Market Participants involved in providing competitive energy services to end-use Customers. The focus of these model business practices is to describe the procedures and processes for establishing the operational and business relationships between Market Participants thus enabling them to work together in a more consistent and effective manner in competitive electric and natural gas markets.

These model business practices are voluntary and do not address policy issues that are the subject of state legislation or regulatory decisions. These model business practices have been adopted with the realization that as the industry evolves, additional and amended model business practices may be necessary. Any industry participant seeking additional or amended model business practices (including principles, definitions, data elements, process descriptions, and technical implementation instructions) should submit a request to the NAESB office, detailing the change, so that the appropriate process may take place to amend the model business practices.

Business Processes and Practices

RXQ.1 Overview

RXQ.1.1 Principles

- RXQ.1.1.1** The Governing Documents developed for a given geographical market area should be comprehensive and consistent with one another so that all Market Participants have a clear understanding of their roles and obligations.
- RXQ.1.1.2** Role definition should include not only the processes and functions to be performed, but also a description of interactions and communications necessary among Market Participants to enable the market to function efficiently.
- RXQ.1.1.3** All parties should strive to maximize flexibility while minimizing the number and complexity of Governing Documents.
- RXQ.1.1.4** Performance standards should be established for key processes and transactions to ensure that all parties fulfill their roles.
- RXQ.1.1.5** A testing/certification process, as defined in the Governing Documents, is desirable to ensure that new entrants to a market are qualified to perform their roles.

RXQ.1.2 Definitions

- RXQ.0.2.1 Applicable Regulatory Authority:** The state regulatory agency or other local governing body that provides oversight, policy guidance, and direction to any parties involved in the process of providing energy to retail access Customers through regulations and orders.
- RXQ.0.2.3 Assumption of Receivables:** The payment processing method in which the Billing Party assumes the Non-Billing Party's receivables and sends the Non-Billing Party payment at predetermined intervals for all Non-Billing Party amounts that are billed, payable to the Non-Billing Party, and do not have a status of In Dispute, in accordance with the tariff, Billing Services Agreement or other Governing Document regardless of when (or whether) the Customer pays the Billing Party.
- RXQ.0.2.4 Bill Ready:** A Consolidated Billing practice in which the Billing Party receives the calculated charge amount(s) directly from the Non-Billing Party in lieu of the Billing Party calculating it directly from the rate.

- RXQ.0.2.5 Billing Party:** The party performing billing services for one or more parties.
- RXQ.0.2.6 Billing Services Agreement:** A legally binding document between the Distribution Company and the Supplier used when one of the parties is performing Consolidated Billing for the other party. Such document sets forth the expectations and responsibilities of each party.
- RXQ.0.2.12 Consolidated Billing:** The billing option in which the Distribution Company or Supplier renders a Customer bill consolidating the energy, transmission / transportation and distribution charges of the Distribution Company and the Supplier, for which a single payment from the Customer is expected.
- RXQ.0.2.16 Customer:** Any entity that takes gas and/or electric service for its own consumption.
- RXQ.0.2.17 Distribution Company:** A regulated entity which provides distribution services and may provide energy and/or transmission/transportation services in a given area.
- RXQ.0.2.18 Distribution Company Operational Manuals:** Documents prepared and published by Distribution Companies that describe, in detail the operating processes/procedures used to perform retail access functions.
- RXQ.0.2.19 Distribution Company-Supplier Service Agreement:** A bilateral contractual agreement between the Distribution Company and the Supplier that determines the parties' roles, responsibilities, and interactions in serving retail access Customers. Usually this will be the master agreement that will cover most aspects of providing retail access service. There may be one or more subsidiary agreements, covering specific functional areas.
- RXQ.0.2.22 Governing Documents:** Documents that determine the interactions among parties, including, but not limited to, regulatory documents (e.g., tariffs, rules, regulations), contractual agreements, and Distribution Company Operational Manuals.
- RXQ.0.2.27 Market Participant:** A party engaged in the process of providing competitive retail energy to end-use customers including, but not limited to, the Distribution Company, the Supplier, the Registration Agent, the settlement agent, and the meter reading entity.

- RXQ.0.2.28 Market Participant Service Agreements:** All contractual agreements between or among Market Participants that determine the parties' roles, responsibilities, and interactions in serving retail access Customers. These include the Distribution Company-Supplier Service Agreement and any other agreements executed by Market Participants to facilitate retail access (e.g. a contract between a meter reading entity, the Distribution Company, and the Supplier detailing how usage data will be provided).
- RXQ.0.2.30 Non-Billing Party:** The party whose charges are being combined into a statement (or invoice) prepared and rendered by another party.
- RXQ.0.2.35 Registration Agent:** An entity facilitating switches and performing record-keeping for a specified geographical area.
- RXQ.0.2.39 Supplier:** Persons engaged in the competitive sale of energy to end-users.
- RXQ.0.2.41 Switch Request:** A request from a Supplier to switch a Customer to begin receiving service from that Supplier.
- RXQ.0.2.42 Uniform Electronic Transaction:** Standard data arrangements for trading information, making business requests and exchanging other information, encompassing a number of electronic media and utilizing specified transport protocols.
- RXQ.0.2.43 Trading Partner Agreement:** A legally binding agreement between any two Market Participants defining each party's expectations and responsibilities for doing business with each other using Uniform Electronic Transactions.

RXQ 1.3 Model Business Practices

RXQ 1.3.1 Governing Documents

RXQ.1.3.1.1 Typically, the following operational items are addressed in the Governing Documents:

- General
 - Any fees or charges
 - Creditworthiness
 - Standard operating rules
 - Performance standards
 - Dispute resolution process
 - Uniform Electronic Transactions
- Customer Enrollment/Switching
 - Release of Customer information
 - Switching processes and procedures
 - Customer authorization
- Customer Billing and Payment Processing
 - Meter reading and data management
 - Customer billing
 - Customer payment processing
 - Customer credit and collection processes and procedures
- Customer Service
 - Customer service processes and procedures
- Settlement
 - Energy losses
 - Load profiles
 - Scheduling processes and procedures
 - Retail settlement

RXQ.1.3.2 Regulatory Documents

RXQ.1.3.2.1 Market Participants will utilize regulatory documents established by the Applicable Regulatory Authority to provide the policy framework for retail access, including the following:

- All fees and/or credits required for regulated services,
- Definitions of roles and responsibilities, including what has to be done, by when and by whom,
- Definitions of regulatory policy in such areas as: available metering and billing options, creditworthiness standards, and load profiling eligibility.

RXQ.1.3.3 Contractual Agreements

RXQ.1.3.3.1 Market Participants should execute contractual agreements with one another to establish the legal relationship and obligations between the parties in providing retail access service to Customers.

RXQ.1.3.3.2 At a minimum, the Distribution Company and the Supplier should execute a Distribution Company-Supplier Service Agreement encompassing, either directly or through subsidiary agreements, all aspects of providing retail access service where these parties depend upon one another.

RXQ.1.3.3.3 To the extent that some functions required for retail access service are performed by third parties, other than a Distribution Company or Supplier, this third party should execute Market Participant Service Agreements with the Distribution Company or Supplier, as applicable, for the service(s) provided.

RXQ.1.3.3.4 If applicable, Market Participants should also execute:

- Trading Partner Agreements and
- Billing Services Agreements

RXQ.1.3.3.5 In addition to specifying the roles and responsibilities, the Market Participant Service Agreement should also:

- Define the communication process between the parties,
- Set forth performance expectations,
- Define data required for interactions,
- Specify the optional services, such as billing method or metering options that one party will supply to the other along with the relevant terms and conditions, and
- Define the dispute resolution process.

RXQ.1.3.3.6 The content of contractual agreements between Market Participants should adhere to the policies of the Applicable Regulatory Authority.

RXQ.1.3.4 Distribution Company Operational Manuals

RXQ.1.3.4.1 Detailed Distribution Company processes and procedures regarding retail access not covered in regulatory documents or contractual agreements should be stated in Distribution Company Operational Manuals.

RXQ.1.3.4.2 Operational manuals should be nondiscriminatory and publicly available.

RXQ.1.3.4.3 The content of Distribution Company Operational Manuals should adhere to the policies set in regulatory documents and applicable contractual agreements. Where required, the Distribution Company Operational Manuals should be approved by the Applicable Regulatory Authority.

RXQ.1.3.5 Performance Standards

RXQ.1.3.5.1 Performance standards should be developed for key retail access processes and should be published in the Governing Documents.

RXQ.1.3.5.2 Market performance should be monitored, compared to these standards, and appropriate actions taken to achieve performance that meets the standards.

RXQ.1.3.5.3 Performance standards should be:

- nondiscriminatory;
- publicly available;
- collaboratively developed and modified; and
- acknowledged by the Applicable Regulatory Authority.

RXQ.1.3.5.4 Performance standards may be considered for the following operational items, as well as others:

- Customer Information Exchange
 - Customer information request responses issued within the appropriate time frame (indication of problems accessing and/or transmitting Customer information).
- Customer Switching
 - Rejected Switch Requests (indication of problems obtaining necessary validation data from Customer and/or passing data from Supplier to Distribution Company);
 - Customer notification letters issued within the appropriate time frame (indication that Customers are notified of switching activity in time to take action if appropriate);
 - Customer rescissions (indication of Customer confusion, misinformation, and/or unauthorized switching); and
 - Switch responses to valid Switch Requests (or drop responses to valid drop requests) within specified time frame (indication of degree of automation and/or accuracy of switching systems and ability to implement Customer choices).
- Meter Usage and Meter Attributes Data Transfer
 - Time frame for providing meter data (indication of degree of automation and/or accuracy of meter data management systems); and
 - Acceptable levels of estimated/missing data (indication of degree of automation and/or accuracy of meter reading and meter data management systems).

- Billing
 - Required turnaround of Bill Ready charges (indication of problems receiving, calculating and/or transmitting bill-ready billing information within the billing window);
 - Consolidated bills issued with all appropriate charges (indication that Customers are receiving timely and accurate consolidated bills); and
 - Amount of time to render bills after receipt of the Non-Billing Party charges (indication that consolidated bills are issued promptly).
- Payments
 - Customer payments provided by the Billing Party to the Non-Billing Party within an appropriate time frame (indication of problems exchanging cash transactions between the parties); and
 - Assumption of Receivables payments made by the Billing Party to the Non-Billing Party within the appropriate time frame (indication of problems exchanging cash transactions between the parties).

RXQ.1.3.6 Supplier Certification

RXQ.1.3.6.1 Distribution Companies should have a process to certify a Supplier's, or other Market Participant's, ability to perform the roles required of them in that Distribution Company's service area.

RXQ.1.3.6.2 Distribution Companies should apply the certification process in a non-discriminatory manner to all parties who have met all statutory/regulatory requirements for the relevant jurisdiction (e.g. if Supplier licensing is required, a license has been obtained).

RXQ.1.3.6.3 Certification requirements should be met prior to enrolling customers (if a Supplier) or prior to providing a service (other Market Participants providing services such as meter reading or billing).

RXQ.1.3.6.4 Key elements of certification include:

- Demonstrating the ability to exchange data and conduct business via the Uniform Electronic Transactions that have been developed for use in the jurisdiction.
- Demonstrating the ability to handle reasonably expected volumes of transactions accurately while meeting performance standards applicable to the market area.

RXQ.1.3.6.5 Certification requirements should be publicly available so that all potential Market Participants know what is expected.

RXQ.1.3.6.6 Demonstrations of required abilities should include, but are not limited to, nondiscriminatory tests resulting in the successful transfer of funds and/or test data.

RXQ 1.4 Models

The following model agreements can be found in RXQ.6 – Contracts:

- RXQ.6.2 Outline of a Non-Disclosure Agreement**
- RGQ.6.3 Distribution Supplier Service Agreement Outline**
- REQ.6.3 Distribution Supplier Service Agreement Outline**

CREDITWORTHINESS

Executive Summary

The focus of these Creditworthiness Model Business Practices is the procedures and processes for establishing the credit relationship between Distribution Companies and Suppliers to enable them to work together to serve Customers participating in competitive electric and natural gas markets. The procedures and processes described in these model business practices apply to credit risks existing between a Supplier and a Distribution Company in the course of serving Customers, including one or more of the following:

- Risks associated with one party voluntarily (i.e., not when required by the Applicable Regulatory Authority) doing the billing and receiving payments for the other party when Consolidated Billing is utilized;
- Risks associated with the Supplier's purchase of distribution services for resale to its Customers under Single Retail Supplier Billing;
- Risks associated with the Distribution Company being the party that provides replacement energy when a Supplier defaults; and
- Risks associated with receiving payment for other services one party provides another.

The components of the Creditworthiness Model Business Practices are:

Determination of Risk Exposure
Determination of Initial Credit Limit
Reconsideration of Determination of Credit Limit
Disqualification/Remedies
Security Instruments
Calling on Security
Confidentiality

Introduction

The North American Energy Standards Board (NAESB) is a voluntary non-profit organization comprised of members from all aspects of the natural gas and electric industries. Within NAESB, the Retail Electric Quadrant (REQ) and the Retail Gas Quadrant (RGQ) focus on issues impacting the retail sale of energy to end-use Customers. REQ / RGQ model business practices are intended to provide guidance to Distribution Companies, Suppliers, and other Market Participants involved in providing competitive energy services to end-use Customers. The focus of these model business practices is to describe the procedures and processes for establishing the credit relationship between Distribution Companies and Suppliers to enable them to work together to serve Customers participating in competitive electric and natural gas markets.

These model business practices are voluntary and do not address policy issues that are the subject of state legislation or regulatory decisions. These Model Business Practices have been adopted with the realization that as the industry evolves, additional and amended model business practices may be necessary. Any industry participant seeking additional or amended model business practices (including principles, definitions, data elements, process descriptions, and technical implementation instructions) should submit a request to the NAESB office, detailing the change, so that the appropriate process may take place to amend the model business practices.

Business Process and Practices

RXQ.2 Overview

RXQ.2.1 Principles

- RXQ.2.1.1** Creditworthiness procedures should be efficient to minimize the time and effort required by the parties to start and/or maintain a working relationship.
- RXQ.2.1.2** General information concerning the evaluation process and methodology for determining credit limits and risk exposure should be reflected in one or more of the applicable Governing Documents.
- RXQ.2.1.3** The procedures and criteria used to perform a re-evaluation of creditworthiness should be the same as used for the initial determination.
- RXQ.2.1.4** The definition of a Business Day should be defined in the Governing Documents and should be made publicly available, as appropriate.

RXQ.2.2 Definitions

- RXQ.0.2.1 Applicable Regulatory Authority:** The state regulatory agency or other local governing body that provides oversight, policy guidance, and direction to any parties involved in the process of providing energy to retail access Customers through regulations and orders.
- RXQ.0.2.2 Applicant:** The party seeking credit from another party.
- RXQ.0.2.5 Billing Party:** The party performing billing services for one or more parties.
- RXQ.0.2.7 Business Day:** As defined in the Governing Documents.
- RXQ.0.2.8 Cash Deposit:** Money provided by one party to the other to secure performance of an agreement or compensate for possible loss or damage.
- RXQ.0.2.9 Certificate of Authority:** A document attesting to the name(s) and signature(s) of the officer(s) authorized to execute a particular instrument.
- RXQ.0.2.10 Challenge:** The Applicant's request for a review of the Creditor's creditworthiness determination made shortly after that determination.

- RXQ.0.2.11 Confidential Information:** Nonpublic information concerning the financial condition of the Applicant, or any of the Applicant's affiliates, that is disclosed to the Creditor by or on behalf of the Applicant or Applicant's affiliates.
- RXQ.0.2.12 Consolidated Billing:** The billing option in which the Distribution Company or Supplier renders a Customer bill consolidating the energy, transmission / transportation and distribution charges of the Distribution Company and the Supplier, for which a single payment from the Customer is expected.
- RXQ.0.2.13 Credit Application Form:** The Creditor's form for obtaining identification and financial data about an Applicant.
- RXQ.0.2.14 Creditor:** The party granting credit to another party.
- RXQ.0.2.15 Cure Period:** A period of time specified in a contract allowing a defaulting party to rectify the default, during which time the Creditor would not be allowed to exercise its remedies.
- RXQ.0.2.16 Customer:** Any entity that takes gas and/or electric service for its own consumption.
- RXQ.0.2.17 Distribution Company:** A regulated entity which provides distribution services and may provide energy and/or transmission/transportation services in a given area.
- RXQ.0.2.20 Dual Billing:** The billing option in which the Distribution Company and the Supplier, each assuming the role of a Billing Party, render separate Customer bills, each containing charges for the energy, transmission/transportation or distribution services provided by that party, for which separate payments from the Customer are expected.
- RXQ.0.2.21 Event-driven Reconsideration:** A re-evaluation of an Applicant's creditworthiness performed in response to a Material Change in its credit rating or financial condition.
- RXQ.0.2.22 Governing Documents:** Documents that determine the interactions among parties, including, but not limited to, regulatory documents (e.g., tariffs, rules, regulations), contractual agreements, and Distribution Company operational manuals.
- RXQ.0.2.23 Guarantor:** The issuer of a Guaranty.
- RXQ.0.2.24 Guaranty:** An obligation to pay the unpaid obligations of a third party Applicant to a Creditor upon certain conditions being met.

- RXQ.0.2.26 Letter of Credit:** A letter issued by a bank authorizing the beneficiary to draw up to a stated amount of money from the issuing bank, its branches, or other associated banks or agencies, provided that the drawing conditions of the letter are met.
- RXQ.0.2.29 Material Change:** Any change in the Applicant's (or Guarantor's) financial or other condition that might reasonably affect the amount of credit extended to that Applicant or may impact the Applicant's ability to perform on its obligations.
- RXQ.0.2.30 Non-Billing Party:** The party whose charges are being combined into a statement (or invoice) prepared and rendered by another party.
- RXQ.0.2.31 Pay As You Get Paid:** The payment processing method in which the Billing Party forwards payment to the Non-Billing Party for the Non-Billing Party charges only after receiving payment.
- RXQ.0.2.32 Prepayment:** Money provided by one party to the other to pay for goods or services not yet rendered.
- RXQ.0.2.36 Security Interest in Collateral:** A right, title, claim, or share in assets that exists by contract as security for payment or performance of an obligation that is acceptable to the creditor.
- RXQ.0.2.38 Single Retail Supplier Billing:** The billing option in which the Supplier renders a Customer bill for all energy, transmission/transportation, and distribution related charges. The Supplier purchases or otherwise acquires energy, transmission/ transportation and distribution services, and therefore all charges on the bill are Supplier charges. A single payment from the Customer is expected.
- RXQ.0.2.39 Supplier:** Persons engaged in the competitive sale of energy to end-users.
- RXQ.0.2.40 Surety Bond:** An obligation of a third party that covers payments to the Creditor in the event that the Applicant fails to meet its obligations.
- RXQ.0.2.41 Switch Request:** A request from a Supplier to switch a Customer to begin receiving service from that Supplier.

RXQ.2.3 Model Business Practices

RXQ.2.3.1 Overall

RXQ.2.3.1.1 Either the Supplier or the Distribution Company may take on the role of Applicant or Creditor.

RXQ.2.3.1.2 The Applicant should provide the Creditor with the telephone number, e-mail address, facsimile number and mailing address of up to two authorized representatives who are designated to receive creditworthiness communications. The Creditor should provide comparable information to the Applicant. Both the Applicant and the Creditor should promptly notify the other party of any changes in this information. Both parties should manage internal distribution of communications that are received.

RXQ.2.3.1.3 General information concerning the evaluation process and methodology for calculating credit exposure for various risks should be publicly available so that Applicants have access to the requirements prior to making their application.

RXQ.2.3.2 Determination of Risk Exposure

RXQ.2.3.2.1 The credit exposure should be based on the dollar amount determined to be at risk and the period of time during which it remains at risk.

RXQ.2.3.2.2 The same criteria and methodology for calculating credit exposure should be used for all Applicants presenting similar risks, such as the risk associated with Consolidated Billing or the risks associated with providing replacement energy when a Supplier defaults.

RXQ.2.3.2.3 Specific methodologies should be developed, where applicable, for each of the major types of risks that incorporate the dollar amount at risk and the period of time it remains at risk.

For Consolidated Billing, issues may include, but are not limited to:

- Total dollar amount billed;
- Whether the Billing Party assumes the Non-Billing Party's receivables or the Pay As You Get Paid method is employed; and
- When assuming receivables, typical Customer payment behavior (dollars past due, percent late, percent uncollectable, etc.).

For risks associated with the Distribution Company providing replacement energy when a Supplier defaults, issues may include, but are not limited to:

- Responsibilities if a Supplier defaults;
- Amount of load served by the defaulting Supplier; and
- Cost of replacement energy.

For services one party provides to another, issues may include, but are not limited to:

- Total dollar amount for such services ; and
- Payment terms.

RXQ.2.3.3 Determination of Initial Credit Limit

RXQ.2.3.3.1 The initial credit determination, including credit limits, should be established using the same criteria and methodology for all Applicants presenting similar risks, such as the risk associated with Consolidated Billing or the Distribution Company providing replacement energy when a Supplier defaults. The Creditor may consider other exposure from the Applicant beyond the specific credit limit being requested.

RXQ.2.3.3.2 Determination of the amount of credit to extend to a particular Applicant may be based on Applicant-Creditor agreement,

regulatory policy, or other Governing Documents, and may include both secured and unsecured components.

RXQ.2.3.3.3 The Creditor should make available to all Applicants a Credit Application Form that includes a list of required supporting financial documents.

RXQ.2.3.3.4 The Applicant should submit to the Creditor the completed Credit Application Form and one set of the required supporting financial documents.

RXQ.2.3.3.5 The Applicant should submit the Credit Application Form and supporting documents using a method that verifies that delivery took place, such as requiring a signature or requesting a return receipt.

RXQ.2.3.3.6 The Creditor should evaluate the Applicant's Credit Application Form and all supporting financial documents for completeness and notify the Applicant of any missing elements within five (5) Business Days of receipt. Such notification should be in writing and specify the elements needed to complete the application. The notice should be delivered by overnight delivery, facsimile, or e-mail.

RXQ.2.3.3.7 Timelines for processing a creditworthiness evaluation should begin when the Credit Application Form, complete with all required supporting documents, is received by the Creditor.

RXQ.2.3.3.8 The supporting financial documents submitted with the Credit Application Form should cover a two-year period and include the most recent quarter for which financial data is available.

RXQ.2.3.3.9 The Applicant may present evidence of its rating level from a recognized rating agency(ies).

RXQ.2.3.3.10 Supporting financial documents may include:

- Two most recent annual reports;
- Most recent SEC Form 10-K and 10-Q and any independent auditor's letter to management or, if SEC Form 10-K is unavailable, substitute audited annual financial information (including a balance sheet, income statement, cash flow statement with notes, and any independent auditor's letter to management);
- Most recent quarterly or monthly financial information (including a balance sheet, income statement, and cash flow statement with notes) accompanied by all attestations required by the SEC that the information submitted is true, correct and a fair representation of Applicant's financial condition; and
- For private companies the year-end financials should be independently audited by a licensed Certified Public Accountant and include any notes to the financial statements and debt schedules. These documents should be accompanied by an attestation by the chief executive officer, chief financial officer or the owner that the information submitted is true, correct and a fair representation of Applicant's current financial condition.

RXQ.2.3.3.11 When the creditworthiness requirement is being met through a Guaranty, the creditworthiness requirements that apply to the Applicant also apply to the Guarantor. In addition to submitting supporting financial documents, the Guarantor should provide documentation of the Guaranty, as applicable.

For a Parental Guaranty:

- Certificate of Authority of the individual signing the contract and/or ancillary documents; and
- Board resolution or bylaws demonstrating that the Guarantor can guarantee this type of transaction for the Applicant.

For a Third-Party Guaranty:

- Certificate of Authority of the individual signing the contract and/or ancillary documents;
- Board resolution or bylaws demonstrating that the Guarantor can guarantee this type of transaction for the Applicant; and
- Agency agreement, acceptable to the Creditor, that ties the Guarantor to the Applicant.

For a Foreign Guarantor:

- Certificate of Authority of the individual signing the contract and/or ancillary documents;
- Board resolution, or equivalent (e.g., Articles of Association/Organization), with a copy of the bylaws demonstrating that the Guarantor has the authority to enter into such a Guaranty; and
- Legal opinion that states a judgment for the Creditor would be enforceable in the country of the Guarantor.

RXQ.2.3.3.12 The Creditor should complete the creditworthiness evaluation within ten (10) Business Days of receipt of all required documents.

RXQ.2.3.3.13 The Creditor should provide the results of the creditworthiness evaluation to the Applicant in writing within five (5) Business Days of completing the evaluation. The results should be delivered by overnight delivery, facsimile, or e-mail. The notice should include the rationale for the determination of the risk exposure and credit limits.

RXQ.2.3.4 Reconsideration of Determination of Credit Limit

RXQ.2.3.4.1 An Applicant should be granted an opportunity to challenge a credit limit determination. The Challenge should be submitted within thirty (30) calendar days of receiving the written notification of the credit limit determination.

RXQ.2.3.4.2 The Creditor should respond to a timely Challenge within five (5) Business Days of receipt by providing rationale for its determination. The Creditor should also review with the Applicant the data used as input to ensure there were no errors or missing data that impacted the result. If there were material errors or omissions, the Creditor should re-evaluate the Applicant's creditworthiness within ten (10) Business Days of receipt of corrected information. The Creditor should provide the results of the creditworthiness re-evaluation to the Applicant in writing within five (5) Business Days of completing the re-evaluation. The results should be delivered by overnight delivery, facsimile, or e-mail. The notice should include the rationale for the determination of the risk exposure and credit limits.

RXQ.2.3.4.3 If the Applicant remains dissatisfied with the outcome of the creditworthiness evaluation by a Creditor who is regulated, it may elevate its Challenge to the Applicable Regulatory Authority, as applicable.

RXQ.2.3.4.4 An Applicant should notify the Creditor of any adverse Material Change in its financial condition within three (3) Business Days of such change.

RXQ.2.3.4.5 A Creditor may periodically re-evaluate the creditworthiness of an Applicant and also when it becomes aware of an adverse Material Change in the Applicant's financial condition.

RXQ.2.3.4.6 An Applicant may request an Event-Driven Reconsideration when there has been a favorable Material Change in its financial status, such as an upgrading by a major bond rating agency. Such reconsideration will be treated as a new credit application.

RXQ.2.3.4.7 In addition to Event-Driven Reconsiderations, an Applicant may request a re-evaluation of its creditworthiness no more than once every twelve months. Such re-evaluation will be treated as a new credit application.

RXQ.2.3.5 Disqualification/Remedies

RXQ.2.3.5.1 Whenever the Creditor's risk exposure exceeds the amount covered by the Applicant's security arrangements, the Creditor may require additional security appropriate to the amount of additional risk exposure.

RXQ.2.3.5.2 Whenever the Creditor's risk exposure becomes less than the amount covered by the Applicant's security arrangements, the Creditor should comply with the Applicant's request for a reduction in the security held, appropriate to the amount of risk exposure.

RXQ.2.3.5.3 Requests for security, additional security or reduction of security should be in writing and delivered by overnight delivery, facsimile, or e-mail.

RXQ.2.3.5.4 When a Creditor requests security and the required security is not tendered within the period specified in the appropriate Governing Documents, the Creditor may begin taking actions to reduce its exposure, as allowed under the Governing Documents, including, but not limited to:

- (If the Applicant is a Supplier) Cease processing any Switch Requests that add to the Customers served by the Applicant;
- Moving any of the Applicant's Customers currently on Applicant Consolidated Billing to Dual Billing, effective on the Customer's next normally scheduled bill;
- Reducing the sales of any other products or services the Creditor may have been making to the Applicant until the credit exposure no longer exceeds the Applicant's credit limit; and/or
- Taking remedial action, including disqualification of the Applicant, as allowed by the Applicable Regulatory Authority.

RXQ.2.3.5.5 When the Applicant is a Supplier and it can partially, but not fully, meet a request for security in the time period specified in the appropriate Governing Documents, it can avoid disqualification by reducing the risk exposure it presents to the Distribution Company to an amount commensurate with the amount of security tendered.

RXQ.2.3.6 Security Instruments

RXQ.2.3.6.1 Creditors should offer the option of one or more of the following forms of secured credit to those Applicants who do not qualify for sufficient unsecured credit for the risks that they present.

- Cash Deposit
- Guaranty
- Letter of Credit
- Prepayment
- Security Interest in Collateral
- Surety Bonds

Such forms of secured credit should be acceptable to the Creditor and the Creditor's acceptance should not be unreasonably withheld. The Creditor and Applicant may mutually agree that the Applicant will provide other forms of security.

RXQ.2.3.7 Calling on Security

RXQ.2.3.7.1 The Creditor may call upon the security posted by the Applicant as specified in applicable agreements or tariffs, or after all of the following occur:

- Written notice of default is provided to the Applicant; and
- Payment or other action to cure the default is not made within the Cure Period.

RXQ.2.3.7.2 The same criteria and methodology for establishing the appropriate length of the Cure Period should be used for all Applicants presenting similar risks, such as the risk associated with Consolidated Billing or an entity acting as the party that provides replacement energy when a Supplier defaults.

RXQ.2.3.7.3 The Creditor may call upon the security posted by the Applicant without prior notice if the Applicant files a petition for bankruptcy (or equivalent, including the filing of an involuntary petition in bankruptcy against the Applicant).

RXQ.2.3.7.4 A Distribution Company acting as the Creditor may immediately call upon the security posted by the Applicant (that is a Supplier) without prior notice if the Applicant for any reason ceases to provide energy service to all of its Customers within the Distribution Company's service territory (i.e. the Supplier has effectively withdrawn from the market).

RXQ.2.3.8 Confidentiality

RXQ.2.3.8.1 The Confidential Information provided to the Creditor in the creditworthiness evaluation process should be used only for the purpose of establishing the Applicant's financial status in order to enable the parties to enter into contracts for the products/services to be provided. The Confidential Information should not be publicly disclosed, except as required by the Applicable Regulatory Authority.

RXQ.2.3.8.2 When entering into the creditworthiness evaluation process the Applicant and the Creditor should execute a non-disclosure agreement, if requested by the Applicant, unless non-disclosure is provided for within other Governing Documents.

RXQ.2.3.8.3 Conditions under which a Creditor may disclose Confidential Information to a third party should be covered in a non-disclosure agreement or other Governing Documents.

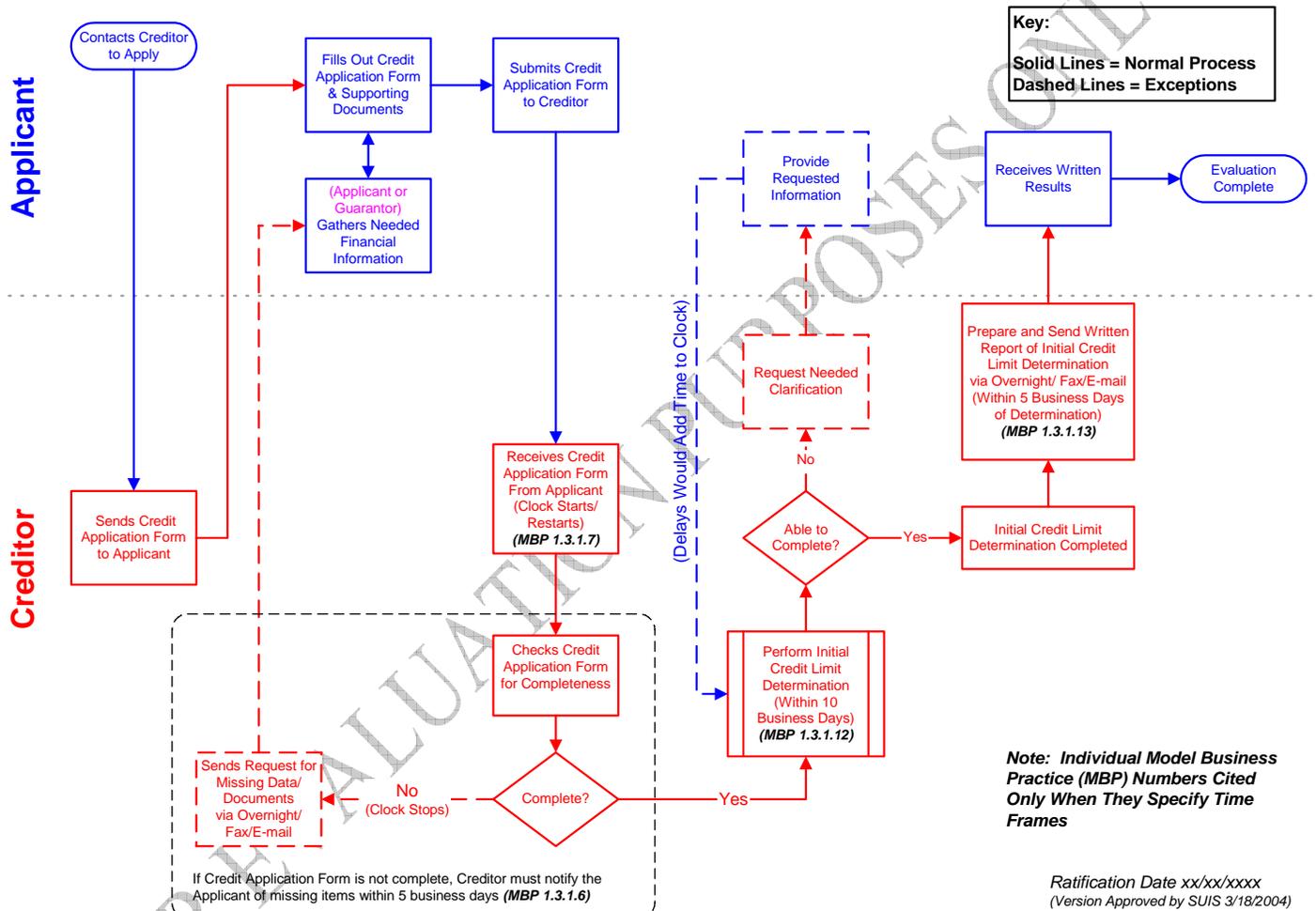
FOR EVALUATION PURPOSES ONLY

RXQ.2.4 Models

RXQ.2.4.1 Determination of Initial Credit Limit – Process Flow

Determination of Initial Credit Limit - Process Flow

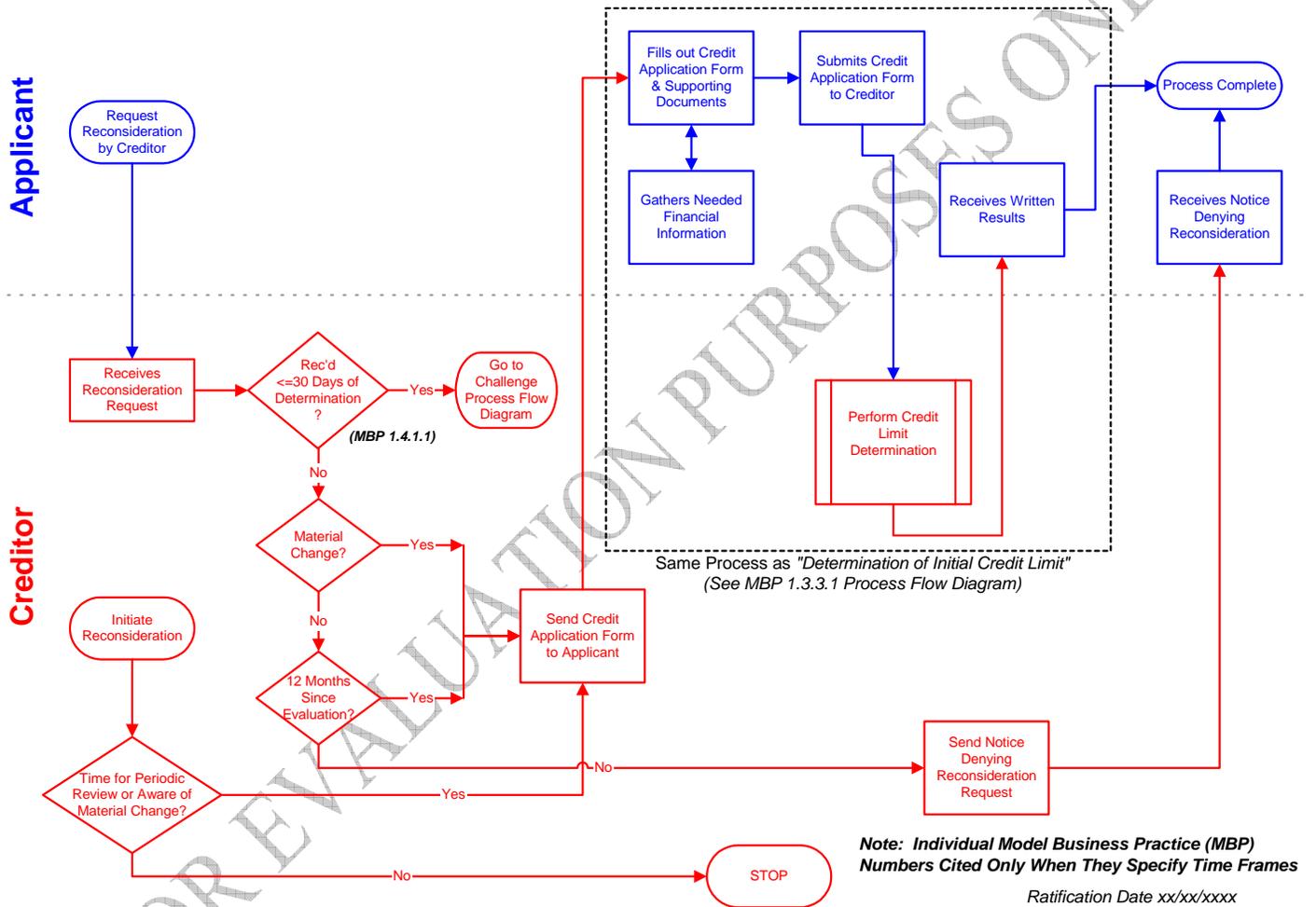
Creditworthiness Evaluation Process (Section 1.3.3.1)



RXQ.2.4.2 Reconsideration of Determination Initial Credit Limit - Process Flow

Reconsideration of Determination of Initial Credit Limit - Process Flow

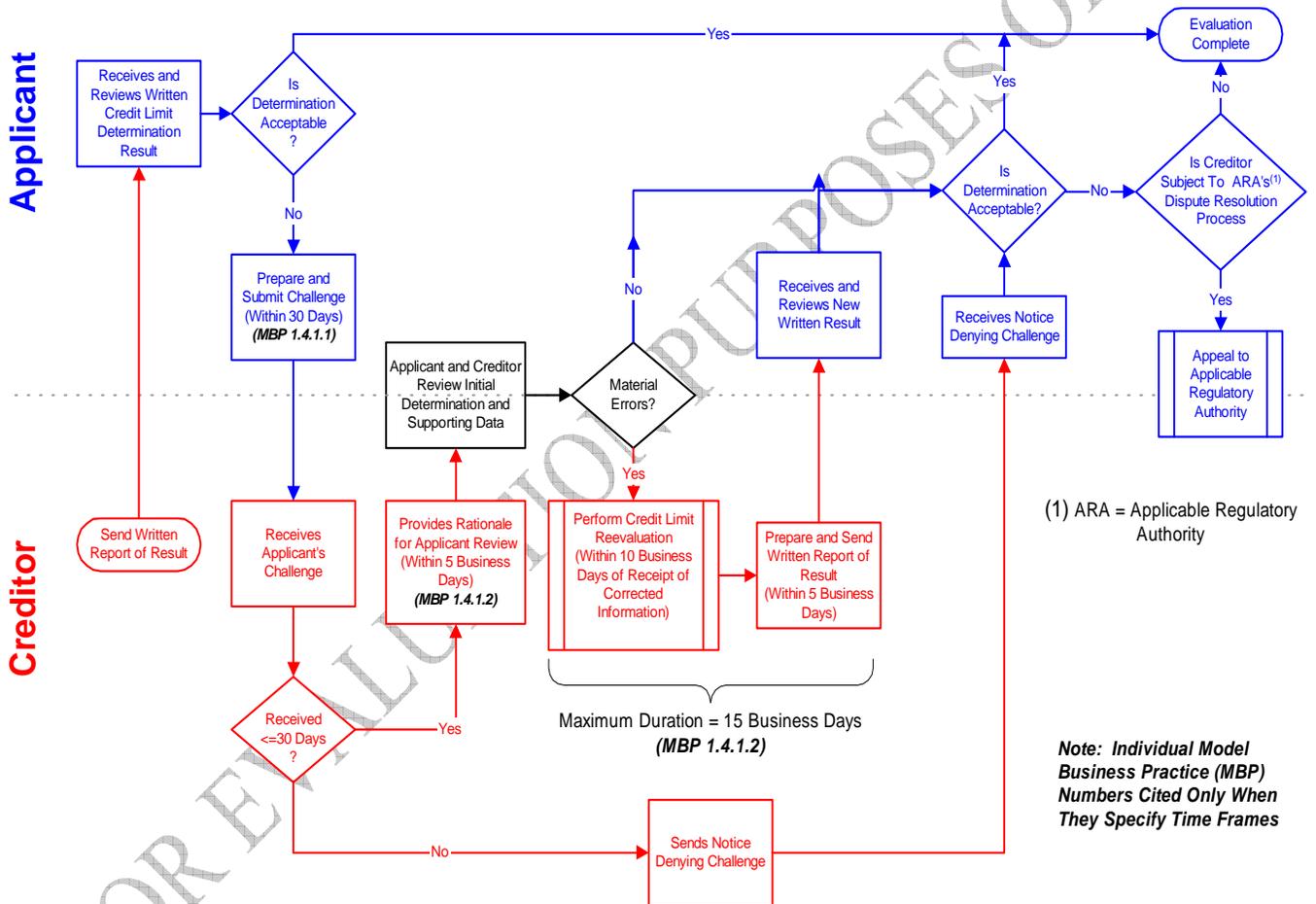
Creditworthiness Evaluation Process (Section 1.4.3.1)



RXQ.2.4.3 Reconsideration of Determination of Initial Credit Limit – Challenge Process Flow

Reconsideration of Determination of Initial Credit Limit - Challenge Process Flow

Creditworthiness Evaluation Process (Section 1.4.3.2)

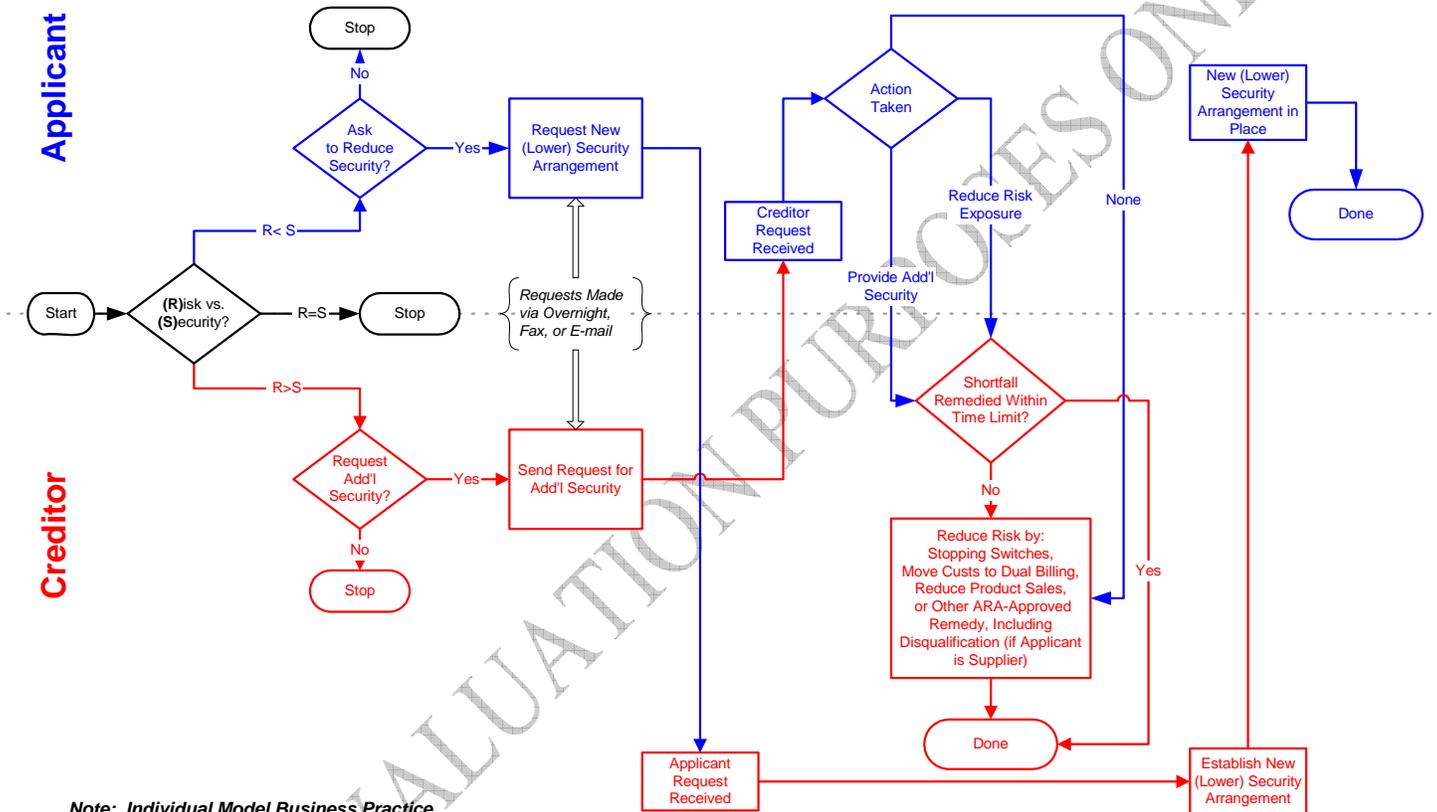


Ratification Date xx/xx/xxxx
(Version Approved by SUIS 3/18/2004)

RXQ.2.4.4 Disqualification/Remedies – Process Flow

Disqualification/Remedies - Process Flow

Disqualification/Remedies (Section 1.5.3.1)



Note: Individual Model Business Practice (MBP) Numbers Cited Only When They Specify Time Frames

Ratification Date xx/xx/xxxx
(Version Approved by SUIS 3/18/2004)

BILLING and PAYMENTS

Executive Summary

This section presents a summary of the business practices for billing and payment processing in competitive electric and natural gas markets where alternative energy providers, known as Suppliers, sell natural gas or electricity to end use Customers. The Supplier provides the energy by purchasing or producing it and arranges for its delivery by the Distribution Company to the retail Customer.

Billing and payment processing encompasses a variety of interactions between the meter reading entity, the Billing Party and the Non-Billing Party. Interactions include the transfer of data necessary to accurately bill and process payments received from the Customer for energy, transmission/transportation and distribution related charges. In a business environment where best practices are voluntary, model business practices should be applied within the context of regulatory requirements and agreements between the parties documented in a Billing Services Agreement. The primary steps are:

- The usage data is obtained;
- Charges are calculated for both the energy and transmission/transportation and distribution charges based on the same Customer usage for the period;
- Charges are billed to the Customer
 - Dual Billing
 - Consolidated Billing
 - Supplier Consolidated Billing-Bill Ready
 - Supplier Consolidated Billing-Rate Ready
 - Distribution Company Consolidated Billing-Bill Ready
 - Distribution Company Consolidated Billing-Rate Ready
 - Single Retail Supplier Billing
- Payments are collected from the Customer;
- Payments are forwarded to the Non-Billing Party when Consolidated Billing is used;
 - Assumption of Receivables
 - Pay As You Get Paid

Introduction

The North American Energy Standards Board (NAESB) is a voluntary non-profit organization comprised of members from all aspects of the natural gas and electric industries. Within NAESB, the Retail Electric Quadrant (REQ) and the Retail Gas Quadrant (RGQ) focus on issues impacting the retail sale of energy to end-use customers. REQ / RGQ Model Business Practices are intended to provide guidance to Distribution Companies, Suppliers, and other Market Participants involved in providing competitive energy service to end-use Customers. The focus of these Model Business Practices is the processing of billing and payment transactions.

These Model Business Practices are voluntary and do not address policy issues that are the subject of state legislation or regulatory decisions. These Model Business Practices have been adopted with the realization that as the industry evolves, additional and amended Model Business Practices may be necessary. Any industry participant seeking additional or amended Model Business Practices (including principles, definitions, data elements, process descriptions, and technical implementation instructions) should submit a request to the NAESB office, detailing the change, so that the appropriate process may take place to amend the Model Business Practice.

Business Processes and Practices

RXQ.3 Overview

RXQ.3.1 Principles

RXQ.3.2 Definitions

- RXQ.0.2.1 Applicable Regulatory Authority:** The state regulatory agency or other local governing body that provides oversight, policy guidance, and direction to any parties involved in the process of providing energy to retail access Customers through regulations and orders.
- RXQ.0.2.3 Assumption of Receivables:** The payment processing method in which the Billing Party assumes the Non-Billing Party's receivables and sends the Non-Billing Party payment at predetermined intervals for all Non-Billing Party amounts that are billed, payable to the Non-Billing Party, and do not have a status of In Dispute, in accordance with the tariff, Billing Services Agreement or other Governing Document regardless of when (or whether) the Customer pays the Billing Party.
- RXQ.0.2.4 Bill Ready:** A Consolidated Billing practice in which the Billing Party receives the calculated charge amount(s) directly from the Non-Billing Party in lieu of the Billing Party calculating it directly from the rate.
- RXQ.0.2.5 Billing Party:** The party performing billing services for one or more parties.
- RXQ.0.2.6 Billing Services Agreement:** A legally binding document between the Distribution Company and the Supplier used when one of the parties is performing Consolidated Billing for the other party. Such document sets forth the expectations and responsibilities of each party.
- RXQ.0.2.7 Business Day:** As defined in the Governing Documents.
- RXQ.0.2.12 Consolidated Billing:** The billing option in which the Distribution Company or Supplier renders a Customer bill consolidating the energy, transmission / transportation and distribution charges of the Distribution Company and the Supplier, for which a single payment from the Customer is expected.

- RXQ.0.2.16 Customer:** Any entity that takes gas and/or electric service for its own consumption.
- RXQ.0.2.17 Distribution Company:** A regulated entity which provides distribution services and may provide energy and/or transmission/transportation services in a given area.
- RXQ.0.2.20 Dual Billing:** The billing option in which the Distribution Company and Supplier render separate Customer bills for the products and services each provides.
- RXQ.0.2.22 Governing Documents:** Documents that determine the interactions among parties, including but not limited to: regulatory documents (e.g., tariffs, rules, regulations), contractual agreements, and Distribution Company operational manuals.
- RXQ.0.2.25 In Dispute:** A bill status that prevents collection action from being taken on the disputed amount.
- RXQ.0.2.27 Market Participant:** A party engaged in the process of providing competitive retail energy to end-use customers including but not limited to the Distribution Company, the Supplier, the Registration Agent, the settlement agent, and the meter reading entity.
- RXQ.0.2.30 Non-Billing Party:** The party whose charges are being combined into a statement (or invoice) prepared and rendered by another party.
- RXQ.0.2.31 Pay As You Get Paid:** The payment processing method in which the Billing Party forwards payment to the Non-Billing Party for the Non-Billing Party charges only after receiving payment.
- RXQ.0.2.33 Rate Code:** A product identifier used in a billing system which contains all information, such as description and price, needed to bill for that product. One or more Rate Codes may be billed on a single account.
- RXQ.0.2.34 Rate Ready:** Refers to the practice in which the Non-Billing Party provides rate information to the Billing Party sufficient to calculate the Non-Billing Party's charges.
- RXQ.0.2.35 Registration Agent:** An entity facilitating switches and performing record keeping for a specified geographical area.

RXQ.0.2.37 Service Delivery Point: A physical metered and/or unmetered service location supplying energy to a Customer premise.

RXQ.0.2.38 Single Retail Supplier Billing: The billing option in which the Supplier renders a Customer bill for all energy, transmission/transportation, and distribution related charges. The Supplier purchases or otherwise acquires energy, transmission/transportation and distribution services, and therefore all charges on the bill are Supplier charges. A single payment from the Customer is expected.

RXQ.0.2.39 Supplier: Persons engaged in the competitive sale of energy to end-users.

RXQ.0.2.42 Uniform Electronic Transaction: Standard data arrangements for trading information, making business requests and exchanging other information, encompassing a number of electronic media and utilizing specified transport protocols.

RXQ.3.3 Model Business Practices

RXQ.3.3.1 General Billing and Payment

RXQ.3.3.1.1 The Supplier may elect to offer its Customers one or more of the billing options that are available in the Distribution Company's territory.

RXQ.3.3.1.2 Both Distribution Company and Supplier should be approved, certified or licensed, to the extent required by the Applicable Regulatory Authority and demonstrate the technical capability to exchange information electronically using Uniform Electronic Transactions and to meet the operational time frames which have been defined to support the billing options required.

RXQ.3.3.1.3 The Supplier should provide adequate advance notice to the Distribution Company if it plans to implement another available, approved billing option. Such option should not become operational until proof of successful data interchange is demonstrated to the satisfaction of both parties and all requirements are met.

RXQ.3.3.1.4 When making changes to its billing or payment systems that may affect electronic data interchange, the Supplier or Distribution Company making those changes should

provide advance notice to the other party prior to implementation.

RXQ.3.3.1.5 Required metering data that are necessary to fulfill billing responsibilities should be made available to all appropriate party(s) via Uniform Electronic Transactions.

RXQ.3.3.1.6 Applicable state and local taxes will be calculated, collected, and remitted in accordance with state statutes and local government ordinances.

RXQ.3.3.1.7 The cancel and re-bill process should be clear and reproducible, and be communicated to all affected parties.

RXQ.3.3.2 Dual Billing

RXQ.3.3.2.1 The Distribution Company and the Supplier each acts as a Billing Party and should independently produce and render separate bills directly to the Customer in accordance with the requirements set by the Applicable Regulatory Authority.

RXQ.3.3.2.2 The Customer should make two separate payments; one to the Distribution Company and one to the Supplier.

RXQ.3.3.2.3 When meter usage is cancelled:

- Usage for all applicable periods should be cancelled by metering period; and
- The usage sent in the cancellation transaction should match the usage sent in the original transaction.

RXQ.3.3.2.4 When meter usage is restated:

- Usage for all applicable periods should be restated by metering period; and
- Unless there has been a product or rate change, the restated usage transaction should be sent at the same level of detail as the original usage transaction.

RXQ.3.3.3 Consolidated Billing - General

- RXQ.3.3.3.1** Either the Distribution Company or the Supplier should assume the role of either Billing Party or Non-Billing Party provided that applicable regulatory or legal criteria are met.
- RXQ.3.3.3.2** The Billing Party and Non-Billing Party should execute a Billing Services Agreement. The responsibilities of the parties, performance parameters, financial arrangements and other details associated with payment processing and remittance should be set forth in the Billing Services Agreement.
- RXQ.3.3.3.3** The Billing Party should render a consolidated bill in accordance with the requirements set by the Applicable Regulatory Authority and any agreements set forth in the Billing Services Agreement.
- RXQ.3.3.3.4** When the Supplier is the Billing Party it should be responsible for delivering to Customers bill enclosures or bill messages containing Non-Billing Party related information that is mandated by the Applicable Regulatory Authority.
- RXQ.3.3.3.5** When a consolidated bill is rendered there should be one Customer payment due date.

RXQ.3.3.4 Consolidated Billing - Bill Ready Billing

- RXQ.3.3.4.1** The Billing Party should receive the Non-Billing Party's billing information via Uniform Electronic Transaction within two (2) Business Days following the meter reading entity's transmission of valid usage information.
- RXQ.3.3.4.2** When the Non-Billing Party files are received, the Billing Party should acknowledge receipt of a file via Uniform Electronic Transaction within one (1) Business Day of receipt of the file.
- RXQ.3.3.4.3** If, upon examination, it is determined that the Non-Billing Party's file cannot be processed then the Billing Party should reject it. Rejection, accompanied by appropriate uniform error code(s), should be communicated via the appropriate Uniform Electronic Transaction within one (1) Business Day of receipt of the file.

RXQ.3.3.4.4 If the Non-Billing Party's transaction is accepted, the Billing Party should bill the Customer(s) within two (2) Business Days of receipt of such transaction.

RXQ.3.3.4.5 When the Billing Party is able to process the Non-Billing Party's transactions but is unable to render a significant number of Customer bills within two (2) Business Days of receipt of the Non-Billing Party's charges, the Billing Party should promptly notify the Non-Billing Party.

RXQ.3.3.4.6 If the Non-Billing Party's transactions are received within the appropriate time frame and a transaction is rejected, then the Billing Party should notify the Non-Billing Party of the rejection accompanied by appropriate uniform error code(s), via Uniform Electronic Transaction within one (1) Business Day of receipt of such transaction. The Non-Billing Party may, if time permits, submit a file containing corrected transactions for inclusion in the current bill.

RXQ.3.3.4.7 If the Non-Billing Party's transactions are sent to the Billing Party outside the appropriate time frame such that charges could not be included on the bill, then, as specified in the Billing Services Agreement, the Billing Party should do one of the following:

- Reject the transaction and notify the Non-Billing Party within two (2) Business Days via Uniform Electronic Transaction that the charges were not billed. In this scenario, the Non-Billing Party should resubmit its charges in the following billing period in accordance with the time requirements, or
- Hold the transaction for processing on the next bill and notify the Non-Billing Party that charges were received late and will be reflected on the next bill.

RXQ.3.3.4.8 If the Billing Party's errors cause the Non-Billing Party's charges to miss the billing window and the bill has been issued, the Billing Party should cancel and reissue the bill as soon as practicable, unless the Billing Party and Non-Billing Party arrange a mutually agreeable alternative bill correction process.

- RXQ.3.3.4.9** When a Bill Ready consolidated bill is to be cancelled:
- Usage for all applicable periods should be cancelled by metering period; and
 - The usage sent in the cancellation transaction should match the usage sent in the original transaction.

- RXQ.3.3.4.10** When a cancelled Bill Ready consolidated bill is to be re-billed:
- Usage for all applicable periods should be restated by metering period. Unless there has been a product or rate change, the restated usage transaction should be sent at the same level of detail as the original usage transaction; and
 - The Billing Party should receive the Non-Billing Party's restated billing information within two (2) Business Days following the transmission of valid restated usage information.

- RXQ.3.3.4.11** Both the Billing Party and the Non-Billing Party should be responsible for the calculation of their late payment charges, if applicable, unless directed otherwise by the Applicable Regulatory Authority or as specified in the Billing Services Agreement. The Billing Party should be responsible for placing these charges on the bill.

- RXQ.3.3.4.12** When the Non-Billing Party calculates and assesses late payment charges it should send notification of such charges to the Billing Party via Uniform Electronic Transaction.

RXQ.3.3.5 Consolidated Billing - Rate Ready Billing

- RXQ.3.3.5.1** At least thirty (30) calendar days prior to using a new Rate Code, or as otherwise provided in the Billing Services Agreement, the Non-Billing Party should provide to the Billing Party information needed to establish the new Rate Code.

- RXQ.3.3.5.2** Where the Billing Party's system can accommodate a price change to an existing Rate Code the Non-Billing Party should provide the new price and the requested effective date to the Billing Party at least ten (10) Business

Days prior to the next billing date, or a lesser period of time as provided in the Billing Services Agreement, to allow sufficient time for the Billing Party to implement the change.

RXQ.3.3.5.3 The Billing Party will send a Uniform Electronic Transaction when accounts of the Non-Billing Party are billed thus notifying the Non-Billing Party that its Customers have been billed and indicating the usage and amount so billed for each Customer account.

RXQ.3.3.5.4 When a Rate Ready consolidated bill is to be cancelled:

- Usage for all applicable periods should be cancelled by metering period; and
- The usage sent in the cancellation transaction should match the usage sent in the original transaction.

RXQ.3.3.5.5 When a cancelled Rate Ready consolidated bill is to be re-billed:

- Usage for all applicable periods should be restated by metering period. Unless there has been a product or rate change, the restated usage transaction should be sent at the same level of detail as the original usage transaction;
- The Billing Party should re-bill the Customer by applying the proper usage and proper Billing and Non-Billing Party Rate Code(s) as necessary to correct the previously rendered bill; and
- After the cancel/re-bill event has taken place, the Billing Party should transmit notice of restated usage and the credit, debit, or the net amount, to the Non-Billing Party so that the accounts receivable of the Customer will be properly stated.

RXQ.3.3.5.6 The Billing Party should calculate late payment charges on behalf of the Non-Billing Party, if applicable, using the same methodology used to calculate its own late payment charges, unless directed otherwise by the Applicable Regulatory Authority or as specified in the Billing Services Agreement. The Billing Party should be responsible for placing these charges on the bill.

RXQ.3.3.6 Single Retail Supplier Billing

- RXQ.3.3.6.1** The Supplier should render its bill in accordance with the requirements set by the Applicable Regulatory Authority.
- RXQ.3.3.6.2** When meter usage is cancelled:
- Usage for all applicable periods should be cancelled by metering period; and
 - The usage sent in the cancellation transaction should match the usage sent in the original transaction.
- RXQ.3.3.6.3** When meter usage is restated:
- Usage for all applicable periods should be restated by metering period; and
 - Unless there has been a product or rate change, the restated usage transaction should be sent at the same level of detail as the original usage transaction.
- RXQ.3.3.6.4** If the Supplier does not receive actual meter reading data on a timely basis, the Supplier may issue a bill based on an estimated reading.
- RXQ.3.3.6.5** After the meter(s) is read or the usage is otherwise determined, the Distribution Company should render an invoice that separately identifies the delivery system charges and billing determinants for each Service Delivery Point or Customer account served by the Supplier. Invoices should be transmitted via Uniform Electronic Transaction.
- RXQ.3.3.6.6** Distribution Company invoices are subject to adjustment due to estimated reads or errors including, but not limited to, arithmetic errors, computational errors, and meter reading errors. The Distribution Company should cancel and re-bill the original invoice that was incorrect.
- RXQ.3.3.6.7** Having assumed the obligation to pay the Distribution Company within the acceptable time frame for amounts owed the Distribution Company, the Supplier should have the flexibility to change billing and payment practices subject only to applicable laws, regulatory requirements,

or as otherwise allowed in any agreement between the parties regarding terms and conditions for energy delivery.

RXQ.3.3.6.8 The Supplier may elect either to accept charges other than usage-based charges or to have the Distribution Company bill those charges directly to the Customer.

RXQ.3.3.7 Payment Processing – Consolidated Billing – General

RXQ.3.3.7.1 If the Non-Billing Party does not receive payment for undisputed charges from the Billing Party within the appropriate time frame, then the Non-Billing Party should send notification to the Billing Party of the interest and/or fees, if any, applicable to the un-remitted amount. Such notification should be sent via Uniform Electronic Transaction and in accordance with the terms and conditions of the Billing Services Agreement or pursuant to the requirements of the Applicable Regulatory Authority. Remittance of interest and/or fees, if any, should be made by electronic means to a financial institution designated by the Non-Billing Party.

RXQ.3.3.7.2 The Billing Party, upon placing the Non-Billing Party's charges In Dispute, should, within one (1) Business Day, notify the Non-Billing Party of the subject and amount In Dispute, in a manner specified in the Billing Services Agreement.

RXQ.3.3.7.3 The Non-Billing Party, upon placing its charges In Dispute, should, within one (1) Business Day, notify the Billing Party of the subject and amount In Dispute, in a manner specified in the Billing Services Agreement.

RXQ.3.3.7.4 Once a dispute is resolved and the charges are no longer In Dispute, the party resolving the dispute should notify the other party of the resolution, in a manner specified in the Billing Services Agreement.

RXQ.3.3.7.5 Where charges have been placed In Dispute, payments should be applied against charges that are not In Dispute first unless otherwise directed by the Applicable Regulatory Authority.

RXQ.3.3.7.6 When there is a change in Billing Party, the Non-Billing Party's balance should not be transferred to the new Billing Party unless mutually agreed upon by all of the affected Billing Parties and Non-Billing Parties.

RXQ.3.3.7.7 If a Customer enters into a multi-month payment arrangement for all or a portion of the bill, it is the responsibility of the party entering into such agreement with the Customer to maintain proper accounting for such transaction. Neither the Billing Party nor the Non-Billing Party should enter into such an agreement for amounts owed to the other party, unless otherwise directed by the Applicable Regulatory Authority or specified in the Billing Services Agreement.

RXQ.3.3.8 Payment Processing – Consolidated Billing – Assumption of Receivables

RXQ.3.3.8.1 The Billing Services Agreement should specify any level of uncollectible revenues to be reflected in the amount due to the Non-Billing Party.

RXQ.3.3.8.2 The Billing Services Agreement should specify any creditworthiness criteria that the Non-Billing Party's Customers would have to satisfy to be eligible for a consolidated bill.

RXQ.3.3.8.3 On or before the date the payment is due to the Non-Billing Party, the Billing Party should send a Uniform Electronic Transaction notifying the Non-Billing Party of account-specific payments to be made. By mutual agreement, the Billing Party may send account-specific information along with the remittance of funds in an electronic certification to the bank in lieu of, or in addition to, direct notification to the Non-Billing Party.

RXQ.3.3.8.4 The Billing Party forwards payment for all undisputed charges to the Non-Billing Party within five (5) Business Days of the due date stated on the Customer's bill or as specified in the Billing Services Agreement.

RXQ.3.3.8.5 The Billing Party remittance of funds should be made by electronic means to a bank designated by the Non-Billing Party.

RXQ.3.3.8.6 In the circumstance where the Distribution Company is the Billing Party, it can reject an enrollment transaction that specifies Consolidated Billing if the Customer does not satisfy the creditworthiness criteria specified in the appropriate Governing Documents. The ability to reject an enrollment transaction may be subject to the requirements of the Applicable Regulatory Authority. If the enrollment is rejected for these reasons, the Non-Billing Party may resubmit the enrollment transaction and specify Dual Billing.

RXQ.3.3.8.7 When the Distribution Company is the Billing Party it may initiate conversion of a Customer to Dual Billing or to the applicable regulated energy supply service, in accordance with the Billing Services Agreement and the requirements of the Applicable Regulatory Authority, when a threshold of overdue payments or delinquencies is reached. The following practices should be used:

- Prior to conversion, the Billing Party may notify the Non-Billing Party of the status of overdue payments or delinquencies; and
- In addition to any notice that may be required to be sent to the Customer, the Billing Party should notify the Non-Billing Party, via Uniform Electronic Transaction, of the effective date of the conversion.

RXQ.3.3.8.8 Return of the Customer to Consolidated Billing should be at the discretion of the Billing Party and subject to the creditworthiness criteria set forth in the Billing Services Agreement.

RXQ.3.3.8.9 When Non-Billing Party charges are placed In Dispute under the Assumption of Receivables payment processing method:

- The Billing Party should withhold payment to the Non-Billing Party of the amount In Dispute; or
- If the Billing Party has made payment of the disputed charges, the Billing Party should initiate a Uniform Electronic Transaction to reverse the payment of the disputed charges. The process for addressing negative transactions resulting from the reversal of

payments of disputed charges should be specified in the BSA.

RXQ.3.3.9 Payment Processing – Consolidated Billing – Pay as You Get Paid

- RXQ.3.3.9.1** Each Business Day the Billing Party should process and post funds received.
- RXQ.3.3.9.2** The Billing Party should process payments in accordance with a predetermined payment posting order as established by the Applicable Regulatory Authority or as agreed to in the Billing Services Agreement.
- RXQ.3.3.9.3** Within one (1) Business Day after posting a payment to the Customer's account, the Billing Party should send a Uniform Electronic Transaction notifying the Non-Billing Party of account-specific payments due to be remitted to the Non-Billing Party.
- RXQ.3.3.9.4** The Billing Party should remit to the Non-Billing Party funds associated with Customer payments posted for all undisputed Non-Billing Party charges within two (2) Business Days or as specified within the rules established by the Applicable Regulatory Authority or as agreed to in the Billing Services Agreement. Remittance of funds should be made by electronic means to a financial institution designated by the Non-Billing Party. By mutual agreement between the parties, the Billing Party may send account-specific information with the remittance of funds in an electronic transaction to the financial institution in lieu of, or in addition to, direct notification to the Non-Billing Party.
- RXQ.3.3.9.5** When a Customer's payment that was previously transmitted to the Non-Billing Party is reversed or adjusted by the Billing Party, the Billing Party should adjust the Customer's account accordingly and send notification of the adjustment to the Non-Billing Party via Uniform Electronic Transaction within one (1) Business Day.
- RXQ.3.3.9.6** The Billing Party should maintain a current and past due balance for each active account of the Non-Billing Party.

RXQ.3.3.9.7 The Billing Party should carry forward any inactive Non-Billing Party arrears on a bill, consistent with requirements of the Applicable Regulatory Authority, or as outlined in the Billing Services Agreement. If amounts remain unpaid, the Billing Party should forward a Uniform Electronic Transaction to the Non-Billing Party to return any outstanding arrears as specified in the Billing Services Agreement or as required by the Applicable Regulatory Authority.

RXQ.3.3.10 Payment Processing – Single Retail Supplier Billing

RXQ.3.3.10.1 On or before the date the payment is due to the Distribution Company, the Supplier should send a Uniform Electronic Transaction notifying the Distribution Company of account-specific payments to be made. By mutual agreement, the Supplier may send account-specific information along with the remittance of funds in an electronic certification to the bank in lieu of, or in addition to, direct notification to the Distribution Company.

RXQ.3.3.10.2 The Supplier remittance of funds should be made by electronic means to a bank designated by the Distribution Company.

RXQ.3.3.10.3 If the Distribution Company does not receive payment for undisputed charges from the Supplier within the appropriate time frame, then the Distribution Company should send notification to the Supplier of the interest and/or fees, if any, applicable to the un-remitted amount. Such notification should be sent via Uniform Electronic Transaction and in accordance with the terms and conditions of the Billing Services Agreement or pursuant to the requirements of the Applicable Regulatory Authority. Remittance of interest and/or fees, if any, should be made by electronic means to a financial institution designated by the Distribution Company.

RXQ.3.3.10.4 When there is a change in Supplier, the Customer's balance should not be transferred to the new Supplier.

RXQ.3.4 Models

The following model agreements can be found in RXQ.6 – Contracts:

RXQ.6.4 Billing Services Agreement For Consolidated Billing

FOR EVALUATION PURPOSES ONLY

DISTRIBUTION COMPANY – SUPPLIER DISPUTES

Executive Summary

These Distribution Company – Supplier Disputes Model Business Practices present procedures and processes for resolving disputes between Suppliers and Distribution Companies that may arise in the context of serving Customers participating in competitive electric and natural gas markets. These model business practices provide guidance on the following topics:

- Establishing a documented dispute resolution process
- Initiating of the dispute resolution process
- Responding to disputes
- alternative dispute resolution
- Escalating a dispute to a Court/Applicable Regulatory Authority

These model business practices do not address disputes between the Customer and the Distribution Company or disputes between Customers and Suppliers.

Introduction

The North American Energy Standards Board (NAESB) is a voluntary non-profit organization comprised of members from all aspects of the natural gas and electric industries. Within NAESB, the Retail Electric Quadrant (REQ) and the Retail Gas Quadrant (RGQ) focus on issues impacting the retail sale of energy to end-use Customers. REQ / RGQ model business practices are intended to provide guidance to Distribution Companies, Suppliers, and other Market Participants involved in providing competitive energy services to end-use Customers. The focus of these model business practices is procedures and processes for resolving disputes between Suppliers and Distribution Companies that may arise in the context of serving Customers participating in competitive electric and natural gas markets.

These model business practices are voluntary and do not address policy issues that are the subject of state legislation or regulatory decisions. These model business practices have been adopted with the realization that as the industry evolves, additional and amended model business practices may be necessary. Any industry participant seeking additional or amended model business practices (including principles, definitions, data elements, process descriptions, and technical implementation instructions) should submit a request to the NAESB office, detailing the change, so that the appropriate process may take place to amend the model business practices.

Business Processes and Practices

RXQ.4 Overview

RXQ.4.1 Principles

- RXQ.4.1.1** The Supplier and Distribution Company shall use good faith and commercially reasonable efforts to informally resolve all disputes.
- RXQ.4.1.2** Parties may also pursue other legal mechanisms to address disputes, but are encouraged to use the following practices first.
- RXQ.4.1.3** Neither party should be required to give up its right to seek formal resolution of a dispute except as part of a signed, mutual agreement.

RXQ.4.2 Definitions

- RXQ.0.2.1** **Applicable Regulatory Authority:** The state regulatory agency or other local governing body that provides oversight, policy guidance, and direction to any parties involved in the process of providing energy to retail access Customers through regulations and orders.
- RXQ.0.2.16** **Customer:** Any entity that takes gas and/or electric service for its own consumption.
- RXQ.0.2.17** **Distribution Company:** A regulated entity which provides distribution services and may provide energy and/or transmission/transportation services in a given area.
- RXQ.0.2.19** **Distribution Company-Supplier Service Agreement:** A bi-lateral contractual agreement between the Distribution Company and the Supplier that determines the parties' roles, responsibilities, and interactions in serving retail access Customers. Usually this will be the master agreement that will cover most aspects of providing retail access service. There may be one or more subsidiary agreements, covering specific functional areas.

RXQ.0.2.22 **Governing Documents:** Documents that determine the interactions among parties, including, but not limited to, regulatory documents (e.g., tariffs, rules, regulations), contractual agreements, and Distribution Company Operational Manuals.

RXQ.0.2.39 **Supplier:** Persons engaged in the competitive sale of energy to end-users.

RXQ.4.3 Model Business Practices

RXQ.4.3.1 Dispute Resolution Process

RXQ.4.3.1.1 There should be a single consistent dispute resolution process for all disputes between Suppliers and Distribution Companies.

RXQ.4.3.1.2 The dispute resolution process should be identified in the Distribution Company -Supplier Service Agreement.

RXQ.4.3.1.3 The details of dispute resolution practices can be spelled out in a Governing Document.

RXQ.4.3.1.4 Such Governing Documents should refer to or cite applicable law, remedies, and responsibilities for the cost of frivolous allegations.

RXQ.4.3.1.5 Each Supplier and Distribution Company should provide the name, title, telephone number, e-mail address, facsimile number and mailing address of up to two authorized representatives who are designated to receive and respond to formal disputes under this practice. Both parties should promptly notify the other party of any changes in this information.

RXQ.4.3.1.6 Both parties should manage internal distribution of communications that are received.

RXQ.4.3.2 Initiating the Dispute Resolution Process

RXQ.4.3.2.1 Any Supplier or Distribution Company may initiate the formal dispute resolution process by presenting a written notice of the dispute to the other party(ies) involved in the dispute.

RXQ.4.3.2.2 This notice should be sent using a method that verifies that delivery took place, such as requiring a signature or requesting a return receipt.

RXQ.4.3.2.3 The notice should include:

- a detailed description of the act, omission, or matter generating the dispute, with all supporting documentation, information and data available to the party initiating the dispute;
- specific reference to the Governing Documents that are alleged to have been violated, and the basis for the allegation;
- other factors or matters relevant to the dispute; and
- a proposed resolution.

RXQ.4.3.3 Responding to Dispute

RXQ.4.3.3.1 As soon as possible, but not more than twenty (20) calendar days following receipt of the notice of dispute, the receiving party should provide a written response to the party(ies) that initiated the dispute with:

- An alternative proposal for resolution if the party's(ies)' proposed resolution is deemed unacceptable; or,
- The results of any informal resolution that may have been reached with the other party(ies) prior to that date.

RXQ.4.3.3.2 If the initial exchange of written material (and perhaps verbal discussions) does not resolve the dispute, the party(ies) may request a meeting(s) to discuss the matter further.

RXQ.4.3.3.3 The responding party(ies) should agree to such a meeting(s) to be held within fifteen (15) calendar days following the request.

RXQ.4.3.3.4 At such meeting a timetable for resolving the dispute should be mutually agreed upon beyond which the parties may pursue other remedies subject to the conditions in 4.5.1.1.

RXQ.4.3.4 Alternative Dispute Resolution

RXQ.4.3.4.1 Whenever possible the parties should agree to use an alternative dispute resolution process prior to or in lieu of petitioning the appropriate court or regulatory authority to intervene. This process can reflect mutually agreed-upon time frames that may differ from those defined in the dispute resolution process.

RXQ.4.3.4.2 The parties must mutually agree on the selection of the neutral third party to administer the alternative dispute resolution process.

RXQ.4.3.4.3 The neutral third party administering the alternative dispute resolution process shall be authorized only to interpret and apply the provisions of the applicable Governing Documents and shall have no power to modify or change any of the Governing Documents in any manner.

RXQ.4.3.5 Escalation to Court/Applicable Regulatory Authority

RXQ.4.3.5.1 If a resolution is not obtained within forty-five (45) calendar days after the receipt of the initial dispute letter or the mutually agreed-upon time frame, either party may file the dispute with the appropriate court or Applicable Regulatory Authority for formal resolution.

RXQ.4.3.5.2 If a party believes that special circumstances (such as an emergency involving public safety, system reliability or significant financial risk) exist that would require more expeditious resolution of a dispute than might be expected under the process described here, it may submit its dispute directly to the Applicable Regulatory Authority, with a copy provided to the other party(ies) involved in the dispute.

RXQ.4.3.5.3 Absent agreement to the contrary, nothing shall restrict the rights of any party to file a complaint with the Applicable Regulatory Authority.

FOR EVALUATION PURPOSES ONLY

QUADRANT-SPECIFIC ELECTRONIC DELIVERY MECHANISM

Executive Summary

This North American Energy Standards Board (NAESB) Retail Electric Quadrant (REQ) and Retail Gas Quadrant (RGQ) Quadrant-Specific Electronic Delivery Mechanism (QEDM) Model Business Practice manual details high-level model business practices that apply to all REQ/RGQ (RXQ) electronic delivery business practices.

The QEDM model business practices establish the framework for the electronic dissemination and communication of information between parties in the North American retail gas and electric marketplaces. Specifically, the Retail Electric Quadrant and the Retail Gas Quadrant of the North American Energy Standards Board have standardized several methods of communication that can be implemented. The methods are:

1. EDI/EDM Transfer - The transfer of EDI files, as defined by the ANSI-based NAESB REQ/RGQ file format model business practices, transferred via the Internet using the NAESB Internet Electronic Transport (Internet ET) mechanism.
2. FF/EDM Transfer - The transfer of "flat files", as defined by the NAESB REQ/RGQ file format model business practices, transferred via the Internet using the NAESB Internet ET mechanism.

For each of these areas, this document provides a high-level guide to development, implementation, and testing. This guide is not intended to be a comprehensive, in-depth manual.

Introduction

NAESB is a voluntary, non-profit organization comprised of members from all aspects of the energy industry. Within NAESB, the Retail Electric Quadrant (REQ) and the Retail Gas Quadrant (RGQ) focus on issues impacting the retail sale of energy to end-use customers. REQ/RGQ Model Business Practices are intended to provide guidance to Distribution Companies, Suppliers, and other Market Participants involved in providing competitive energy services to end-use customers. The focus of these Model Business Practices is Electronic Delivery Mechanisms (EDMs).

NAESB Model Business Practices are voluntary and do not address policy issues that are the subject of state legislation or regulatory decisions. NAESB model business practices are written as 'minimums'. A Trading Party may offer to 'exceed the minimum model business practice' by offering additional functions or features as options, but should not require their use. Such additional features or functions are termed "mutually agreed to" in that, if both Trading Partners agree on the inclusion, the additional feature requirements will be met. However, 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 model business practices. NAESB defines 'exceed the minimum model business practice' to mean surpassing the model business practices without negative impact on contracting and non-contracting parties.

All of the model business practices have been adopted with the anticipation that as the industry evolves and uses the model business practices, additional and amended NAESB model business practices will be necessary. Any industry participant seeking additional or amended model business practices (including principles, definitions, model business practices, data elements, process descriptions, technical implementation instructions) should submit a request to the NAESB office detailing the change so that the appropriate process may take place to amend the model business practices. Standards are grouped in books according to activity in the retail market. Each book is organized according to the outline below:

Business Processes and Practices

RXQ.5 Overview

RXQ.5.1 Principles

- RXQ.5.1.1** 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.
- RXQ.5.1.2** RXQ model business practices are not intended to dictate or choose market outcomes.
- RXQ.5.1.3** RXQ solutions should be cost effective, simple and economical.
- RXQ.5.1.4** RXQ solutions should provide for a seamless marketplace for energy.
- RXQ.5.1.5** Electronic communications between parties should be done on a non-discriminatory basis, whether through an agent or directly with any party.
- RXQ.5.1.6** Trading Partners should mutually select and use a version of the NAESB RXQ model business practices under which to operate, unless specified otherwise by the Applicable Regulatory Authority. Trading Partners should also mutually agree to upgrade or adopt later versions of RXQ model business practices as needed, unless specified otherwise by the Applicable Regulatory Authority.
- RXQ.5.1.7** Trading Partners should post clear and precise business processing rules at a designated site, and/or in writing upon request.
- RXQ.5.1.8** For Electronic Delivery Mechanisms (EDM), there should be at least one automated computer-to-computer exchange of transactional data for each defined transaction data exchange format.
- RXQ.5.1.9** For EDM, transaction content and usage should reasonably correspond to defined data dictionaries regardless of mechanism, e.g. FF/EDM, EDI/EDM, etc.
- RXQ.5.1.10** For EDM, automated business processes should use Internet ET.

RXQ.5.2 Definitions

Where there are discrepancies due to editing or maintenance, definitions in this section are official.

RXQ.0.2.1 Applicable Regulatory Authority: The state regulatory agency or other local governing body that provides oversight, policy guidance, and direction to any parties involved in the process of providing energy to retail access Customers through regulations and orders.

RXQ.0.2.43 Batch Flat-file: The automated computer-to-computer transfer of Flat-files.

RXQ.0.2.7 Business Day: As defined in the Governing Documents.

RXQ.0.2.44 Business Rule Change: Any a) change in the presence and/or the acceptable content of a data element sent by the changing party; b) new business response to an accepted data element received by the changing party; c) new business response to the acceptable content of a data element received by the changing party; or d) new intended business result.

RXQ.0.2.45 D-U-N-S® Number: The D-U-N-S® Number is a 9-digit number assigned to companies by the Dun & Bradstreet Corporation .The D-U-N-S+4® Number is a 10- to 13-digit number, where characters 10 through 13 are arbitrarily assigned by the owner of the D-U-N-S® Number.

RXQ.0.2.17 Distribution Company: A regulated entity which provides distribution services and may provide energy and/or transmission/transportation services in a given area.

RXQ.0.2.46 EDI/EDM: Electronic Data Interchange/Electronic Delivery Mechanism. Describes ANSI ASC X.12 computer-to-computer electronic data interchange of information in files as mapped from RXQ.x.4.z model business practices in the NAESB RXQ Implementation Guides and communicated between Trading Partners over the Internet using the NAESB Internet Electronic Transport (ET).

RXQ.0.2.47 Entity: 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 energy transactions.

RXQ.0.2.48 Entity Common Code: The D-U-N-S® or D-U-N-S+4® number

used as the common company identifier. Entity common codes should be 'legal entities,' that is, Ultimate Location, Headquarters Location, and/or Single Location in Dun &Bradstreet terms.

- RXQ.0.2.49 FF/EDM:** Flat File/Electronic Delivery Mechanism. describes a standardized Flat-file electronic data interchange of information in files as mapped from the RXQ.x.4.z model business practices.
- RXQ.0.2.50 Flat-file:** An ASCII comma-separated-value (CSV) file with the characteristics as defined in the RXQEDM model business practices.
- RXQ.0.2.51 Interactive Flat-file:** Describes the FF/EDM transfer of Flat-files using an interactive browser.
- RXQ.0.2.27 Market Participant:** A party engaged in the process of providing competitive retail energy to end-use customers including but not limited to the Distribution Company, the Supplier, the Registration Agent, the settlement agent, and the meter reading entity.
- RXQ.0.2.52 RXQEDM:** Electronic Delivery Mechanism model business practices for the NAESB RGQ and REQ quadrants that govern package payload file contents, including ANSI ASC X.12 EDI, Flat-file and other formats.
- RXQ.0.2.39 Supplier:** Persons engaged in the competitive sale of energy to end-users.
- RXQ.0.2.53 Testing:** Verification that Trading Partners have the system capabilities in place for: a) intended business results, b) proposed electronic transport, including security, enveloping, cryptography; and c) Electronic Delivery Mechanisms (EDI/EDM or FF/EDM), including data validity, model business practice compliance, etc.
- RXQ.0.2.54 Trading Partner:** A party that enters into an agreement with another party to transact business electronically using NAESB model business practices.
- RXQ.0.2.43 Trading Partner Agreement:** A legally binding agreement between any two Market Participants defining each party's expectations and responsibilities for doing business with each other using Uniform Electronic Transactions.

RXQ.0.2.55 Translator: A program or set of programs that process the contents of payloads, applying ANSI ASC X.12 and other model business practices, and transform the information to other formats.

RXQ.5.3 Model Business Practices

RXQ 5.3.1 General Electronic Delivery Mechanism

RXQ.5.3.1.1 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® number at the Branch Location level; OR 2) to accommodate accounting for an entity that is identified at the Branch Location level.

RXQ.5.3.2.1 RXQEDM relies on the NAESB Internet ET to enforce the privacy, authentication, integrity, and non-repudiation (PAIN) security principles.

RXQ.5.3.2.2 All RXQEDM payloads should be encrypted with a minimum 128 bit key when sent on unsecured networks (Internet). This encryption is built into transportation using the NAESB Internet ET. Where other transport options are used, a 128-bit Secure Sockets Layer (SSL) encryption should be used.

RXQ.5.3.2.3 Trading Partners should retain transaction data for at least 24 months for audit purposes or as specified by the Applicable Regulatory Authority.

RXQ.5.3.2.4 Timestamps that indicate the time transactions were received by a party should be the 'time-c' timestamp from the Internet ET Response.

RXQ.5.3.2.5 RGQ and REQ require the use of the Internet ET Response 'time-c-qualifier' data element to identify the time-zone of the Receiver's timestamp.

- RXQ.5.3.2.6** Timestamps used within RXQEDM transactions should be generated using clocks that are synchronized with the localized prevailing National Institute of Standards and Technology (NIST) time to mitigate discrepancies between the clocks of the Sender and Receiver. Computer clocks should be synchronized as often as necessary to ensure a +/- 5 second variance with an atomic clock. Specific business processes may have tighter synchronization requirements.
- RXQ.5.3.2.7** When Internet ET is used, the Internet ET Receipt timestamp supersedes any EDM timestamps with respect to official time the document was received by the Receiver.
- RXQ.5.3.2.8** When Internet ET is not used, the receipt timestamp is defined by each specific EDM.
- RXQ.5.3.2.9** RXQEDM 'date' data elements should be formatted as YYYYMMDD.
- RXQ.5.3.2.10** RXQEDM 'time' data elements should be specified in a 24 hour format, formatted as HH:MM or HH:MM:SS.
- RXQ.5.3.2.11** RXQEDM 'date/time' data elements that have date and time expressed in one data element should be formatted as YYYYMMDD HH:MM or YYYYMMDD HH:MM:SS, with exactly one space between the day (DD) and the hour (HH).
- RXQ.5.3.2.12** Where they exist for the same business function, Flat-files, EDI and other EDMs should use the same nomenclature for data set names, data element names, code values and/or code value descriptions, abbreviations and message text.
- RXQ.5.3.2.13** Trading Partners should use common codes for legal entities for RXQEDM envelope data elements.
- RXQ.5.3.2.14** To the extent that multiple EDMs are used (e.g. EDI or Flat-files), the same business result should occur.
- RXQ.5.3.2.15** Non-NAESB Internet ET packages (e.g. PDF files) will have the 'input-format' tag set to 'PAYLOAD' to indicate the format is found in the payload MIME segment. Inside the MIME segment and the 'content-type' header will be set to an appropriate MIME content type.

RXQ 5.3.3 ANSI X.12 Electronic Data Interchange (EDI/EDM)

- RXQ.5.3.3.1** NAESB is a member of ANSI and will strive to remain fully-compliant with ANSI ASC X.12 standards.
- RXQ.5.3.3.2** EDI Translators generate the ANSI ASC X.12 file, including control numbers and counts that will appear within the ISA/IEA

outer envelope segments, and within the GS/GE inner envelope segments.

- RXQ.5.3.3.3** The ISA is the interchange control segment to be used on all NAESB ANSI ASC X.12 model business practices.
- RXQ.5.3.3.4** The Receiver should send a 997 FA for each X.12 file received.
- RXQ.5.3.3.5** Inbound EDI transactions should be processed every day business is conducted. The 997 should be sent within one day of business, as defined by the Receiver, of the receipt of the X.12 file.
- RXQ.5.3.3.6** When Internet ET is used, the Internet ET receipt timestamp is the official receipt timestamp. Without Internet ET, the 997 timestamp is the official receipt timestamp.
- RXQ.5.3.3.7** RXQEDM uses X.12 Version 4010 standards unless otherwise noted.

RXQ 5.3.4 Flat-File (FF/EDM)

- RXQ.5.3.4.1** FF/EDM records are separated by a carriage return/line feed (CRLF or \r\n or ASCII 10 and 13).
- RXQ.5.3.4.2** The first record of an FF/EDM Flat-file should be the standard abbreviations for RXQ data elements in the order the corresponding data appears in subsequent rows. The data element order is at the option of the sender.
- RXQ.5.3.4.3** If an FF/EDM Flat-file data element abbreviation is not recognized, the entire Flat-file should be rejected.
- RXQ.5.3.4.4** Each transaction (e.g. Enrollment) should be contained in a single FF/EDM Flat-file record.
- RXQ.5.3.4.5** FF/EDM data elements are separated by commas.
- RXQ.5.3.4.6** FF/EDM data elements that may contain a comma should be enclosed by double quotes.
- RXQ.5.3.4.7** FF/EDM data elements should not contain double quotes.
- RXQ.5.3.4.8** FF/EDM data elements that contain negative numbers should have the minus sign precede the number.
- RXQ.5.3.4.9** FF/EDM data elements that contain decimal precision should include the decimal point within the data element.
- RXQ.5.3.4.10** FF/EDM data elements that contain numeric data with one or more significant leading zeros should preserve these zeros within the data element.
- RXQ.5.3.4.11** FF/EDM 'date', 'time', and 'date/time' data elements should

conform to RXQEDM and ISO model business practices:
date=YYYYMMDD, time=HH:MM:SS, date/time=YYYYMMDD
HH:MM:SS.

- RXQ.5.3.4.12** FF/EDM data elements should be no longer than 256 characters.
- RXQ.5.3.4.13** FF/EDM Flat-files should not contain mixed record formats in a single file (e.g. a single file with both Enrollments and Invoices).
- RXQ.5.3.4.14** FF/EDM payloads should be encrypted prior to Internet transport when not using Internet ET. SSL encryption is sufficient.
- RXQ.5.3.4.15** Transactions sent using FF/EDM should produce the same business result as other EDMs (e.g. EDI/EDM).

RXQ 5.5.1 Testing and Deployment

- RXQ.5.5.1.1** When a party implements a Business Rule Change that will apply to documents, changes systems used to process transactions, or changes third-party service providers, it should notify its Trading Partners at least thirty (30) days in advance of the change(s). The notification should identify the nature of the changes being made, the data element(s) that are changing, the intended business result of such change(s) in the business rule(s), and the scheduled effective date of such change(s).
- RXQ.5.5.1.2** Trading Partners implementing changes should provide testing of change(s) prior to the implementation of the change(s).
- RXQ.5.5.1.3** Trading Partners are permitted to cancel or postpone scheduled changes. Notice of cancellation or postponement should be provided to Trading Partners at least one Business Day prior to the scheduled effective date.
- RXQ.5.5.1.4** Trading Partners should use dedicated testing systems that mirror production systems.

Related Model Business Practices

A. INTERNET ELECTRONIC TRANSPORT (ET)

In NAESB business processes, the RXQEDM model business practices are generally used in conjunction with the Internet ET transport model business practices.

Related Definitions from Internet ET

These definitions are used in this document. For exact definitions, please refer to the Internet ET model business practices manual.

- RXQ.0.2.68 'Electronic Package'. A data stream sent via HTTP POST that contains envelope header information and Payload File(s). The Payload Files are encrypted using defined Internet ET encryption techniques.
- RXQ.0.2.75 'Internet EDM'. The GISB and NAESB WGQ standards up to and including Version 1.7. 'Internet ET' standards and 'RXQEDM' model business practices are derived from these EDM standards.
- RXQ.0.2.79 'Exchange Failure'. An exchange failure is when a sending party's NAESB Internet ET server has had three or more protocol failures over a period of time no less than thirty minutes and no more than two hours.
- RXQ.0.2.80 'QEDM'. Quadrant-specific Electronic Delivery Mechanism; the set of standards or model business practices for each NAESB quadrant that define the EDM standards/model business practices for EDI, Flat-files, electronic bulletin boards, and other technologies. The QEDM excludes electronic transport practices and standards. The QEDMs were derived from the GISB and NAESB WGQ Internet EDM standards.
- RXQ.0.2.81 'Receipt'. The HTTP Response sent from the Receiver to the Sender that includes the 'gisb-acknowledge-receipt' section with a timestamp and OK/error status.
- RXQ.0.2.85 'Technical Exchange Worksheet' or 'TEW'. A document or worksheet used to communicate important information related to the technical implementation of Internet ET; includes information such as URLs, contacts and Public Key policies.

Related Standards from Internet ET

- RXQ.7.3.5 A timestamp designates the time a file is received at the Receiver's designated site. The timestamp consists of the 'time-c' data element, and in some cases the 'time-c-qualifier' data element. Refer to QEDM model business practices for use of the 'time-c-qualifier'.

B. ENTITY COMMON CODE

REQ and RGQ use the D-U-N-S® or D-U-N-S®+4® number as the common company identifier for the HTTP Request and Response data dictionary 'to' and 'from' HTTP header elements. The D-U-N-S® number is a 9-digit number assigned to companies by the Dun & Bradstreet Corporation (D&B). The D-U-N-S+4® number is a 10- to 13-digit number, where characters 10 through 13 are arbitrarily assigned by the owner of the D-U-N-S® number.

For RXQEDM Common Code purposes, an entity will use one and only one D-U-N-S® number. Entity Common Codes should be 'legal entities,' that is, Ultimate Location, Headquarters Location, and/or Single Location (in D&B terms). However, in the following situations, a Branch Location (in D&B terms) can also be an Entity Common Code:

1. When the contracting party provides a D-U-N-S® number at the Branch Location level.
2. To accommodate accounting for an entity that is identified at the Branch Location level.

Since D&B offers customers the option of carrying more than one D-U-N-S® number per entity, please refer to NAESB's Web Page for directions on determining the one and only one D-U-N-S® number constituting the NAESB Entity Common Code.

RXQ.5.1.2 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.

*RXQ.5.3.1.1 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® number at the Branch Location level; **OR 2)** to accommodate accounting for an entity that is identified at the Branch Location level.*

C. TRADING PARTNER AGREEMENT

Importance of the Trading Partner Agreement When Using Internet ET and WGQ QEDM

The Trading Partner Agreement (TPA) specifies what functions each party should perform in electronic transactions. The QEDM contains an optional Technical Exchange Worksheet in the appendix that outlines basic QEDM information between trading partners. Additionally, the Internet ET contains an optional Technical Exchange Worksheet that outlines basic connectivity information between trading partners. The specifications in the TPA should be tested before reliance on the production implementation for business transactions.

Technical Implementation

A. GENERAL ELECTRONIC DELIVERY MECHANISM

Open Standards

The “open” technology standards selected by NAESB RXQ are designed to provide flexibility and scalability. The business benefits gained from adherence to open standards are:

- Provides the framework to electronically trade with others (e.g., electric utilities, banks, suppliers, retail customers).
- Encourages marketplace development of off-the-shelf software solutions to support NAESB RXQ QEDM.
- Strengthens security and integrity of electronic communication.

Privacy/Authentication/Integrity/Non-repudiation

RXQ.5.3.2.1 RXQEDM relies on the NAESB Internet ET to enforce the privacy, authentication, integrity, and non-repudiation (PAIN) security principles.

RXQ.5.3.2.2 All RXQEDM payloads should be encrypted with a minimum 128-bit key when sent on unsecured networks (Internet). This encryption is built into transportation using the NAESB Internet ET. Where other transport options are used, a 128-bit Secure Sockets Layer (SSL) encryption should be used.

Audit Trails

RXQ.5.3.2.3 Trading Partners should retain transaction data for at least 24 months for audit purposes or as specified by the Applicable Regulatory Authority.

Receipt Timestamps

Similar to certified postal mail, many Senders are interested in knowing that their document was received, and at what time the document was received. One aspect of ‘non-repudiation’ says that the Receiver cannot deny receiving the document.

The use of an electronic receipt provides the Sender with a level of non-repudiation.

The primary timestamp in NAESB RXQ model business practices is the ‘time-c’ data element found in the ‘gisb-acknowledgement-receipt’ in Internet ET Responses. When Internet ET is used, this timestamp should serve as the primary timestamp for non-repudiation purposes.

When Internet ET is not used, refer to each EDM for the receipt convention. EDI/EDM uses the date and timestamps in the ISA segment. FF/EDM does not have any current timestamp model business practices.

RXQ.5.3.2.4 Timestamps that indicate the time transactions were received by a

party should be the 'time-c' timestamp from the Internet ET Response.

RXQ.5.3.2.5 RGQ and REQ require the use of the Internet ET Response 'time-c-qualifier' data element to identify the time-zone of the Receiver's timestamp.

RXQ.5.3.2.6 Timestamps used within RXQEDM transactions should be generated using clocks that are synchronized with the localized prevailing National Institute of Standards and Technology (NIST) time to mitigate discrepancies between the clocks of the Sender and Receiver. Computer clocks should be synchronized as often as necessary to ensure a +/- 5 second variance with an atomic clock. Specific business processes may have tighter synchronization requirements.

When Internet ET is used, Internet ET timestamps take precedence over EDM timestamps such as those found in the EDI 997. When Internet ET is not used, other timestamps are defined by the EDM (e.g. EDI/EDM or FF/EDM).

RXQ.5.3.2.7 When Internet ET is used, the Internet ET Receipt timestamp supersedes any EDM timestamps with respect to official time the document was received by the Receiver.

RXQ.5.3.2.8 When Internet ET is not used, the receipt timestamp is defined by each specific EDM.

ISO Date and Time Data Elements

RXQEDM data elements should use the following date and time model business practices:

RXQ.5.3.2.9 RXQEDM 'date' data elements should be formatted as YYYYMMDD.

RXQ.5.3.2.10 RXQEDM 'time' data elements should be specified in a 24 hour format, formatted as HH:MM or HH:MM:SS.

RXQ.5.3.2.11 RXQEDM 'date/time' data elements that have date and time expressed in one data element should be formatted as YYYYMMDD HH:MM or YYYYMMDD HH:MM:SS, with exactly one space between the day (DD) and the hour (HH).

Other

RXQ.5.3.2.12 Where they exist for the same business function, Flat-files, EDI and other EDMs should use the same nomenclature for data set names, data element names, code values and/or code value descriptions, abbreviations and message text.

RXQ.5.3.2.13 Trading Partners should use common codes for legal entities for RXQEDM envelope data elements.

Requests for standardization of additional services and/or data elements should be submitted to the appropriate NAESB quadrant Executive Committee.

RXQ.5.3.2.14 To the extent that multiple EDMs are used (e.g. EDI or Flat-files), the same business result should occur.

Internet Electronic Transport for Non-NAESB Packages

RXQEDM supports use of Internet ET for transportation of files other than ANSI ASC X.12 and flat-files. Examples may include reports, load profiles and PDF files. Current Internet ET standards do not accommodate efficient processing of these formats. The following model business practice enables receiving companies to efficiently support these conventions, and eliminates NAESB intervention when a new type of file is to be transmitted.

Non-NAESB payloads sent using RXQEDM model business practices should have the following information in the header:

- Internet ET 'input-format' data element = 'PAYLOAD'. This indicates that the format for the file is found in the MIME payload segment.
- MIME header 'content-type' data element = appropriate MIME content-type.

RXQ.5.3.2.15 Non-NAESB Internet ET packages (e.g. PDF files) will have the 'input-format' tag set to 'PAYLOAD' to indicate the format is found in the payload MIME segment. Inside the MIME segment and the 'content-type' header will be set to an appropriate MIME content type.

B. ANSI ASC X.12 ELECTRONIC DATA INTERCHANGE (EDI/EDM)

ANSI ASC X.12 Standards

RXQ model business practices reflect industry use of the American National Standards Institute (ANSI) ASC X.12 standards maintained by the Data Interchange Standards Association, Inc. (DISA).

Parties using RXQ X.12 EDI standards should have a copy of the ANSI ASC X.12 Standards Reference document for a full understanding of the X.12 requirements. NAESB members may purchase an ANSI reference document through NAESB by contacting the NAESB office. Non-NAESB industry participants may purchase the reference document by contacting the Manager of Publications at DISA (www.disa.org, 703.548.7005)

RXQ EDI technical implementation documents are subsets of ANSI ASC X.12 standards.

RXQ.5.3.3.1 NAESB is a member of ANSI and will strive to remain fully-compliant with ANSI ASC X.12 standards.

Where the X.12 standard does not fully meet a need, NAESB will add interim usages and code values when required. When used, NAESB will submit interim usage/code values to ANSI and the appropriate ANSI organizations for acceptance of the interim solution. ANSI's final solution may provide a usage or code value different from the interim solution. NAESB model business practices will be updated to reflect the final solution.

ANSI ASC X.12 architecture is designed for fully-automated and auditable end-to-end communications.

RXQ.5.3.3.2 EDI Translators generate the ANSI ASC X.12 file, including control numbers and counts that will appear within the ISA/IEA outer envelope segments, and within the GS/GE inner envelope segments.

These numbers and counts are part of the inner and outer envelopes that allow the translator to ensure that all of the segments and all of the data elements have been received and that the transmission was complete.

ISA Outer Envelope

The ISA segment marks the beginning of an X.12 document. It can be equated to an envelope that a paper document would come in via the mail. The envelope may contain one or more 'inner envelope' functional groups (defined by the GS segment) and one or more transaction sets.

RXQ.5.3.3.3 The ISA is the interchange control segment to be used on all NAESB ANSI ASC X.12 model business practices.

The ISA segment identifies the sender and receiver of the document. The Interchange Sender ID/Interchange Receiver ID is published by both the sender and receiver for other parties to use as the sender/receiver ID to route data to them. The

Sender must always code the Sender's ID in the sender element and the designated Receiver's ID in the Receiver ID.

This sender and receiver information is specified in the Technical Exchange Worksheet (TEW) or a Trading Partner Agreement.

There are additional elements in the ISA segment. These elements are traditionally assigned by the sending party's translator. These elements inform the receiver of the date/time that the envelope was generated, the X.12 version number being utilized, whether the transmission is for test or production purposes, and what characters were used to designate the end of a sub element, element or segment.

The ISA also defines characters for the sub element (ISA position 105), element (ISA position 4), and segment delimiters (ISA position 106). These delimiting characters must never appear in the data. The ISA is the only fixed-length X.12 segment as it uses specific positions in the segment to identify the delimiter characters. The Technical Exchange Worksheet (TEW) provides a section for parties to define their default delimiters. However, receiving parties should always check the above ISA positions for EDI/EDM delimiters.

An outer envelope always begins with an ISA segment and ends with an IEA segment.

GS/GE 'Functional Group Header/Trailer' Inner Envelopes

The GS segment indicates the beginning of a functional group and provides control information for the data that follows it. A functional group can be defined as a group of transactions related to one business application. An inner envelope always begins with a GS segment and ends with a GE segment.

An outer envelope may have multiple inner envelopes. For example, within an ISA outer envelope, there may be a GS inner envelope of enrollments and a second GS inner envelope of drops. Each of these inner envelopes is sent within its own GS 'Functional Group Header' and a GE 'Functional Group Trailer'.

The Sender provides the Application Sender's Code that the Receiver will reflect back on acknowledging documents. The Receiver provides the Application Receiver's Code that the Sender will include in the transmission for the Receiver to use in routing to internal applications. Group Control Numbers are originated and maintained by the Sender of the document.

997 'Functional Acknowledgment'

The 997 'Functional Acknowledgment (FA)' transaction set is used to indicate the results of the syntactical analysis of contents of an X.12 file, including the ISA/IEA outer envelope, the GS/GE functional groups, and the transaction sets (ST/SE).

The 997 FA standard covers all of the X.12 and NAESB model business practice criteria that the receiver of the document has incorporated into the receiver's translator. The translator may be set to accept all information into the receiver's application processing, it may be set to accept only ANSI ASC X.12 compliant

information into the receiver's application processing, or it may be set to accept only ANSI ASC X.12 and NAESB compliant information into the receiver's application processing. Compliance checking in a translator may be set to any of several levels. NAESB recommends that compliance checking be set to the element level in the Functional Acknowledgement.

The 997 informs the originator of the transaction whether the translator accepted the file, accepted it with errors, or rejected it. When errors occur, the 997 identifies the location and type of error that was encountered. Once a transaction passes the translator, the 997 is sent to the originator of the transaction and the data (if accepted) is passed on to the receiver's business application for processing.

RXQ.5.3.3.4 The Receiver should send a 997 FA for each X.12 file received.

RXQ.5.3.3.5 Inbound EDI transactions should be processed every day business is conducted. The 997 should be sent within one day of business, as defined by the Receiver, of the receipt of the X.12 file.

The 997 includes a timestamp of when the file was translated.

RXQ.5.3.3.6 When Internet ET is used, the Internet ET receipt timestamp is the official receipt timestamp. Without Internet ET, the 997 timestamp is the official receipt timestamp.

The 4010 version of X.12 standards was the Year 2000 compliant-version of the standards. Note that in this standard the ISA date elements only have a 2-digit year format.

RXQ.5.3.3.7 RXQEDM uses X.12 Version 4010 standards unless otherwise noted.

C. FLAT-FILE (FF/EDM)

The FF/EDM provides a common set of guidelines for the exchange of transactions formatted as a Flat-files.

'Flat-file' is a commonly-used description of files that have records of a single record structure. While Flat-files are almost always text files, text files are not always Flat-files. While comma-separated-value (CSV) files are often Flat-files, they can also be of different record structures.

The NAESB RXQ FF/EDM model business practices attempt to make it easy to create Flat-files using a spreadsheet without significant programming.

FF/EDM Model business practices:

- RXQ.5.3.4.1 FF/EDM records are separated by a carriage return/line feed (CRLF or \r\n or ASCII 10 and 13).*
- RXQ.5.3.4.2 The first record of an FF/EDM Flat-file should be the standard abbreviations for RXQ data elements in the order the corresponding data appears in subsequent rows. The data element order is at the option of the sender.*
- RXQ.5.3.4.3 If an FF/EDM Flat-file data element abbreviation is not recognized, the entire Flat-file should be rejected.*
- RXQ.5.3.4.4 Each transaction (e.g. Enrollment) should be contained in a single FF/EDM Flat-file record.*
- RXQ.5.3.4.5 FF/EDM data elements are separated by commas.*
- RXQ.5.3.4.6 FF/EDM data elements that may contain a comma should be enclosed by double-quotes.*
- RXQ.5.3.4.7 FF/EDM data elements should not contain double-quotes.*
- RXQ.5.3.4.8 FF/EDM data elements that contain negative numbers should have the minus sign precede the number.*
- RXQ.5.3.4.9 FF/EDM data elements that contain decimal precision should include the decimal point within the data element.*
- RXQ.5.3.4.10 FF/EDM data elements that contain numeric data with one or more significant leading zeros should preserve these zeros within the data element.*
- RXQ.5.3.4.11 FF/EDM 'date', 'time', and 'date/time' data elements should conform to RXQEDM and ISO model business practices: date=YYYYMMDD, time=HH:MM:SS, date/time=YYYYMMDD HH:MM:SS.*
- RXQ.5.3.4.12 FF/EDM data elements should be no longer than 256 characters.*
- RXQ.5.3.4.13 FF/EDM Flat-files should not contain mixed record formats in a single file (e.g. a single file with both Enrollments and Invoices).*

RXQ.5.3.4.14 FF/EDM payloads should be encrypted prior to Internet transport when not using Internet ET. SSL encryption is sufficient.

RXQ.5.3.4.15 Transactions sent using FF/EDM should produce the same business result as other EDMs (e.g. EDI/EDM).

D. INTERACTIVE FLAT-FILE (FF/EDM)

No RXQEDM business processes currently use interactive Flat-files.

E. ELECTRONIC BULLETIN BOARD (EBB/EDM)

No RXQEDM business processes currently use electronic bulletin boards.

F. WEB (WEB/EDM)

No RXQEDM business processes currently use web pages.

G. XML (XML/EDM)

No RXQEDM business processes currently use XML.

H. WEB SERVICES (WS/EDM)

No RXQEDM business processes currently use web services.

Testing and Deployment

Testing and deployment is necessary any time a party introduces and updates their systems. Each party determines the level of testing required for a given implementation. In some cases Governing Documents dictate testing requirements.

- RXQ.5.5.1.1 When a party implements a Business Rule Change that will apply to documents, changes systems used to process transactions, or changes third-party service providers, it should notify its Trading Partners at least thirty (30) days in advance of the change(s). The notification should identify the nature of the changes being made, the data element(s) that are changing, the intended business result of such change(s) in the business rule(s), and the scheduled effective date of such change(s).*
- RXQ.5.5.1.2 Trading Partners implementing changes should provide testing of change(s) prior to the implementation of the change(s).*
- RXQ.5.5.1.3 Trading Partners are permitted to cancel or postpone scheduled changes. Notice of cancellation or postponement should be provided to Trading Partners at least one Business Day prior to the scheduled effective date.*
- RXQ.5.5.1.4 Trading Partners should use dedicated testing systems that mirror production systems.*

Additional testing requirements can be found in either A) the Internet ET standard, or B) the specific model business practice for the business process(es) to be implemented.

APPENDICES

A – REFERENCE GUIDE

B – FREQUENTLY ASKED QUESTIONS

C – SAMPLE TECHNICAL EXCHANGE WORKSHEET (TEW)

D – RXQEDM / INTERNET ET 2.0 CROSS-REFERENCE

FOR EVALUATION PURPOSES ONLY

APPENDIX A – REFERENCE GUIDE

NAESB

NAESB Web Site: (www.naesb.org). Primary reference for energy industry standards and model business practices.

Time Synchronization

Time synchronization is required to assure that all Trading Partners' transaction times are accurate. Testing has shown that the clocks on all computer systems drift. 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.

Each NAESB business process may have unique time-synchronization requirements. Refer to the QEDM for time-synchronization model business practices for target markets. Servers need to be time-synchronized according to the standards and model business practices needed for the most-restrictive target market: that is, the one with the smallest drift allowance.

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.

An easy way to obtain the current time is from the U. S. Naval Observatory's Web site at 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, including IETF NTP, Internet daytime, nisttime / usnotime.

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

<http://tycho.usno.navy.mil/ntp.html>
www.ccd.bnl.gov/xntp

Relevant URL's

MIME Standards

RFC 2045: <ftp://ftp.rfc-editor.org/in-notes/rfc2045.txt>

RFC 1767: <ftp://ftp.rfc-editor.org/in-notes/rfc1767.txt>

ASC X.12 Standards

www.x12.org

APPENDIX B – FREQUENTLY ASKED QUESTIONS

Q1: Use of 'time-c-qualifier' across quadrants. We understand that the retail quadrants require the 'time-c-qualifier' for 'gisb-acknowledgement-receipt', while the WGQ does not require this data element. If we participate in multiple quadrants, which standard do we use?

Q2: How do RXQ markets use the 'refnum' and 'refnum-orig' data elements?

Q3: How does RXQEDM support transporting files that do not conform to NAESB model business practices (e.g. load profiles, reports, PDF files, etc)?

Q4: How does this document relate to the Internet ET standard and the model business practices developed for specific business processes (e.g. Billing and Payments)

Q1: Use of 'time-c-qualifier' across quadrants. We understand that the retail quadrants require the 'time-c-qualifier' for 'gisb-acknowledgement-receipt', while the WGQ does not require this data element. If we participate in multiple quadrants, which standard or model business practice do we use?

A: You are required to follow the standards or model business practices dictated by the quadrant that governs the transaction or business process. For example, if you are executing a WGQ nomination, then you should adhere to WGQ standards, which do not require the 'time-c-qualifier'. If you are executing an REQ enrollment, you need to adhere to the REQ model business practices, which require 'time-c-qualifier'. Of course, all parties can mutually-agree to use the 'time-c-qualifier' or not.

Q2: How do RXQ markets use the 'refnum' and 'refnum-orig' data elements?

A: First, these data elements are mutually-agreed, so parties must agree to use these data elements.

The first time you send a package, the two refnum data elements (refnum, refnum-orig) should be identical 40-digit or less integers, unique over time in your systems.

If you do not receive your NAESB response, you should resend the package with a new refnum (again unique over time), and with the refnum-orig equal to the original send of the package.

The refnum data element is always unique over time. The refnum-orig always refers to a refnum that was used in a previous send.

Refnum Example

Package Send	Refnum	refnum-orig
First send	123467890123456	123467890123456
First resend	223467890123457	123467890123456
Second resend	323467890123458	123467890123456

Q3: How does RXQEDM support transporting files that do not conform to NAESB model business practices (e.g. load profiles, reports, PDF files, etc)?

A: First, sending files using RXQEDM that do not conform to NAESB RXQEDM model business practices is supported, though on a mutually-agreed-upon basis. Non-NAESB payloads sent using RXQEDM standards should have the following information in the header:

- Internet ET 'input-format' data element = 'PAYLOAD'. This indicates that the format for the file is found in the MIME payload segment.
- MIME header 'content-type' data element = 'application/consent'. This is the MIME default for 'other' formats.
- MIME header 'content-ID' = [agreed upon name]. This is a text string that defines what type of payload is being sent. For example, ERCOT may send load profile data with this value set to 'ERCOT Load Profile'.

Q4: How does this document relate to the Internet ET standard and the model business practices developed for specific business processes (e.g. Billing and Payments)?

A: RXQEDM model business practices are designed to work in concert with the NAESB Internet ET standards, and with each model business practices book developed by NAESB REQ and RGQ business subcommittees. The table below summarizes the scope of the different documents:

NAESB Standard / Model Business Practice	Scope	
Internet Electronic Transport ([10].y.z)	TCP/IP, HTTP, HTTP POST SSL Encryption OpenPGP/PGP Encryption/Decryption MIME Internet ET Testing	
REQ/RGQ Quadrant-specific Electronic Delivery Mechanism (RXQEDM) (RXQ.5.y.z)	X.12 EDI Conventions Batch Flat-files Interactive Flat-files Electronic Bulletin Board	Informational Postings Web/HTML Web Services XML
Business Process Standards (e.g. Billing, Nominations, etc) (x.3.z)	Data Dictionaries Code Values X.12 Transactions Sets (e.g. 810, 820, etc) XML Schemas Business Process Testing	

APPENDIX C – SAMPLE TECHNICAL EXCHANGE WORKSHEET (TEW)

This appendix recommends data elements that should be exchanged by trading partners when using NAESB RXQ model business practices. These data elements may be included in a technical worksheet profile, or as an exhibit in a TPA.

EDM Specifications	Test	Production
Identify your Entity Common Code / D-U-N-S® /D-U-N-S+4® Number		
Will you send ANSI ASC X.12 EDI/EDM Documents?		
Identify your default EDI/EDM Segment Terminator (character 106 in ISA).		
Identify your default EDI/EDM Data Element Terminator (character 4 in ISA).		
Identify your default EDI/EDM Composite Element Separator (character 105 in ISA).		
Identify your EDI/EDM ISA08/GS08 values.		
Will you send the 'time-c-qualifier' in Receipt? (Y/N)	Y (required by RXQ)	Y (required by RXQ)
Will you send non-NAESB packages ('input-format'='PAYLOAD'; e.g. PDF)?		
List expected 'content-ID' values		

APPENDIX D – RXQEDM / INTERNET ET 2.0 CROSS-REFERENCE

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
RXQ.5.1.1	RXQEDM standards do not pick winners, but rather create an environment where the marketplace can dictate a winner(s).	4.1.2	The Electronic Delivery Mechanism does not pick winners, rather it should create an environment where the marketplace can dictate a winner or winners.	RXQ.7.1.1	The Internet Electronic Transport (ET) does not pick winners, rather it should create an environment where the marketplace can dictate a winner or winners.
RXQ.5.1.2	RXQEDM solutions should be cost effective, simple and economical.	4.1.3	The solutions should be cost effective, simple and economical.	RXQ.7.1.2	Internet ET solutions should be cost effective, simple and economical.
RXQ.5.1.3	RXQEDM solutions should provide for a seamless marketplace for energy.	4.1.4	The solutions should provide for a seamless marketplace for natural gas.	RXQ.7.1.3	Internet ET solutions should provide for a seamless marketplace for energy.
RXQ.5.1.4	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.	4.1.7	Electronic communications between parties to the transaction should be done on a nondiscriminatory basis, whether through an agent or directly with any party to the transaction.	RXQ.7.1.5	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.
RXQ.5.1.5	Trading Partners should mutually select and use a version of the NAESB RXQEDM standards under	4.1.39	Trading Partners should mutually select and utilize a version of the NAESB WGQ EDM standards under which to operate, unless specified	RXQ.7.1.10	Trading Partners should mutually select and use a version of the NAESB Internet ET

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
	which to operate, unless specified otherwise by government agencies. Trading Partners should also mutually agree to upgrade or adopt later versions of RXQEDM standards as needed, unless specified otherwise by government agencies.		otherwise by government agencies. Trading Partners should also mutually agree to adopt later versions of the NAESB WGQ EDM standards, as needed, again unless specified otherwise by government agencies.		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.
RXQ.5.1.6	Market participants should post clear and precise business processing rules at a designated site, and/or in writing upon request.	4.1.9	Service providers should post clear and precise business processing rules at the designated site, or in writing, upon request.		DOES NOT EXIST
RXQ.5.1.7	There should be at least one standard automated computer-to-computer exchange of transactional data for each defined transaction data exchange format.	4.1.10	There should be at least one standard (computer-to-computer exchange of transactional data) for data exchange format.		DOES NOT EXIST
RXQ.5.1.8	Transaction content and usage should reasonably correspond to defined data dictionaries regardless of mechanism, e.g. FF/EDM, EDI/EDM, etc.	4.1.34	For NAESB WGQ FF/EDM, the content and usage of flat files should reasonably correspond to the NAESB WGQ data sets used for NAESB WGQ EDI/EDM.		DOES NOT EXIST
RXQ.5.1.9	Automated business processes should use Internet ET, e.g. FF/EDM, EDI/EDM, etc.	4.1.35	If NAESB WGQ FF/EDM is implemented, flat files should be exchanged via the NAESB WGQ EDI/EDM site or the Customer		DOES NOT EXIST

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
			Activities Web site.		
RXQ.5.2.1	'RXQEDM'. Electric Delivery Mechanism standards for the NAESB RGQ and REQ quadrants that govern package payload file contents, including X.12 EDI, Flat-file and other formats.		DOES NOT EXIST		DOES NOT EXIST
RXQ.5.2.2	"EDI/EDM". The term used to describe ANSI ASC X.12 computer-to-computer electronic data interchange of information in files as mapped from the x.4.z RXQ standards in the NAESB RXQ Implementation Guides and communicated between trading partners over the Internet using the NAESB Internet ET.	4.2.11	"NAESB WGQ EDI/EDM" is the term used to describe ANSI ASC X.12 computer-to-computer electronic data interchange of information in files as mapped from the x.4.z NAESB WGQ standards in the NAESB WGQ Implementation Guides and communicated between trading partners over the Internet using the NAESB WGQ Electronic Delivery Mechanism.		DOES NOT EXIST
RXQ.5.2.3	"Translator". A program or set of programs that process the contents of payloads, applying ANSI ASC X.12 and other standards, and transforms the information to other formats.		DOES NOT EXIST		DOES NOT EXIST
RXQ.5.2.4	'Flat-file'. An RXQEDM Flat-file is an ASCII comma-separated-value (CSV) file with the characteristics as defined in the RXQEDM standards.		DOES NOT EXIST		DOES NOT EXIST
RXQ.5.2.5	'FF/EDM'. The term used to	4.2.12	"NAESB WGQ FF/EDM" is the term		DOES NOT EXIST

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
	describe a standardized flat-file electronic data interchange of information in files as mapped from the x.4.z RXQ standards.		used to describe a standardized flat file electronic data interchange of information in files as mapped from the x.4.z NAESB WGQ standards. NAESB WGQ FF/EDM is communicated between trading partners over the Internet using the NAESB WGQ Electronic Delivery Mechanism.		
RXQ.5.2.6	'Batch Flat-file'. The term used within the FF/EDM to describe the automated computer-to-computer transfer of Flat-files.	4.2.18	"Batch Flat File" is the term used within NAESB WGQ FF/EDM to describe the automated computer-to-computer transfer of flat files.		DOES NOT EXIST
RXQ.5.2.7	'Interactive Flat-file'. The term used within the FF/EDM to describe the transfer of Flat-files using an interactive browser (4.2.19x).	4.2.19	"Interactive Flat File" is the term used within NAESB WGQ FF/EDM to describe the transfer of flat files using an interactive browser.		DOES NOT EXIST
RXQ.0.2.43	'Trading Partner Agreement', or 'TPA' is a legal agreement between trading parties. The TPA often dictates service level agreements and problem remediation processes. The TPA may include QEDM technical exchange information such as ISA numbers, etc.	4.2.26	DOES NOT EXIST	RXQ.0.2.63	'Trading Partner Agreement', or 'TPA' is a legal agreement between trading parties. The TPA often dictates service level agreements and problem remediation processes. The TPA may include technical exchange information such as URLs, et cetera.

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
RXQ.5.2.44	<p>'Business Rule Change'. Any change in: A) the presence and/or the acceptable content of a data element sent by the changing party, B) a new business response to an accepted data element received by the changing party; C) a new business response to the acceptable content of a data element received by the changing party; D) a new intended business result.</p>	4.3.87	<p>When the receiver of: 1) a Nomination, 2) a Pre-determined Allocation, or, 3) a Request for Confirmation, has determined to change the business rule(s) it will apply to the processing of (and/or response to) one or more of these documents; or, when the sender of: 1) a Confirmation Response (solicited and unsolicited), 2) a Scheduled Quantity, 3) a Scheduled Quantity for Operator, 4) an Allocation, 5) a Shipper Imbalance, or, 6) an Invoice has determined to change the business rule(s) it will apply to the generating of (and/or content within) one or more of these documents, then it should notify its trading partners of same at least two weeks in advance of the change(s). The notification should include identification of the data element(s) that are changing (or whose content is changing), the intended business result of such change(s) in the business rule(s), and the effective date of such change(s). For the purposes of this standard, a business rule change is any change in: a) the presence and/or the acceptable content of a data element which is received by the trading partner sending notice; b) a new business response to an accepted data element which is received by the trading</p>		DOES NOT EXIST

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
			<p>partner sending notice; c) a new business response to the acceptable content of a data element which is received by the trading partner sending notice; or, d) a new intended business result to be communicated to a receiver by the trading partner sending notice; Absent mutual agreement between the affected trading partners to the contrary, trading partners notifying their sending or receiving trading partners of a change(s) under this standard should provide the means to test such change(s) during at least a two week time period prior to the effective date of the change(s). Trading partners receiving notice of such change(s) from their trading partner should be prepared not to implement such change(s) even after testing has been completed, as the notifying trading partner is permitted to cancel or postpone such change(s). Notifying trading partners canceling or postponing the effective date of change(s) should provide affected trading partners with notice of cancellation or postponement at least one business day prior to the applicable effective date.</p>		

FOR EVALUATION PURPOSES ONLY

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/Interpretation	ET	Internet ET 2.0
RXQ.5.2.53	Testing between trading partners includes testing of: (A) intended business results, (B) proposed electronic transport, including security, enveloping, cryptography; and (C) electronic delivery mechanisms (xxx/EDM), including data validity, standards compliance, etc.	4.2.20	Testing data sets between trading partners includes testing of: 1. intended business results, 2. proposed electronic delivery mechanisms, and 3. related EDI/EDM and, where supported, FF/EDM implementation issues. Testing should include enveloping, security, data validity, and standards compliance (e.g. ANSI ASC X.12 and NAESB WGQ EDM Related Standards).	RXQ.0.2.56	'Internet ET Testing'. Testing electronic packages between trading partners includes testing of: A) Connectivity; B) Encryption/Decryption; and C) Digital signatures where appropriate.
RXQ.5.3.1	RXQEDM relies on the NAESB Internet ET to enforce the privacy, authentication, integrity, and non-repudiation (PAIN) security principles.		DOES NOT EXIST		DOES NOT EXIST
RXQ.5.3.10	RXQEDM 'time' data elements should be specified in a 24 hour format, formatted as HH:MM or HH:MM:SS.	4.3.80	NAESB WGQ FF/EDM flat files should be formatted as ASCII comma separated value (CSV) files. This means: Rows are separated by a carriage return/line feed (CRLF). Fields are separated by commas. When a field contains a comma, the field should be enclosed by double-quotes. Double-quotes should not be used within any data field. When numeric data is negative, the minus sign should precede the number. When numeric data contains decimal precision, the decimal point should be included within the field. When numeric data contains one or more significant leading zeros, these zeros		DOES NOT EXIST

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/Interpretation	ET	Internet ET 2.0
			<p>should be preserved in the flat file. Date fields should be formatted as YYYYMMDD. Time fields should be specified in a 24 hour format, formatted as HH:MM or HH:MM:SS, as applicable. Date/Time fields should be formatted as YYYYMMDD HH:MM or YYYYMMDD HH:MM:SS when date and time are expressed in one NAESB WGQ data element. Note that there should be exactly one space between the day (DD) and the hour (HH). The maximum amount of data to be placed in a field should be limited to 256 characters. When a field contains no data, the empty field should result in two delimiters next to each other. Note that there should be no blank spaces between the delimiters.</p>		
RXQ.5.3.11	<p>RXQEDM 'date/time' data elements that have date and time expressed in one data element should be formatted as YYYYMMDD HH:MM or YYYYMMDD HH:MM:SS, with exactly one space between the day (DD) and the hour (HH).</p>	4.3.80	<p>NAESB WGQ FF/EDM flat files should be formatted as ASCII comma separated value (CSV) files. This means: Rows are separated by a carriage return/line feed (CRLF). Fields are separated by commas. When a field contains a comma, the field should be enclosed by double-quotes. Double-quotes should not be used within any data field. When numeric data is negative, the minus sign should precede the number. When numeric data contains decimal precision, the decimal point should be</p>		DOES NOT EXIST

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
			<p>included within the field. When numeric data contains one or more significant leading zeros, these zeros should be preserved in the flat file. Date fields should be formatted as YYYYMMDD. Time fields should be specified in a 24 hour format, formatted as HH:MM or HH:MM:SS, as applicable. Date/Time fields should be formatted as YYYYMMDD HH:MM or YYYYMMDD HH:MM:SS when date and time are expressed in one NAESB WGQ data element. Note that there should be exactly one space between the day (DD) and the hour (HH). The maximum amount of data to be placed in a field should be limited to 256 characters. When a field contains no data, the empty field should result in two delimiters next to each other. Note that there should be no blank spaces between the delimiters.</p>		
RXQ.5.3.12	<p>Where they exist for the same business function, Flat-files, EDI and other EDMs should use the same nomenclature for data set names, data element names, code values and/or code value descriptions, abbreviations and message text.</p>	4.3.47	<p>Where they exist for the same business function, flat files and EDI should use the same nomenclature for data set names, data element names, code values and/or code value descriptions, abbreviations and message text. Corresponding Web pages should use data set names, data element names, code value descriptions, abbreviations and message text that correspond to those</p>		DOES NOT EXIST

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
			used in flat files and EDI, where they exist.		
RXQ.5.3.13	Trading partners should use common codes for legal entities for RXQEDM envelope data elements.	4.3.56	The industry should use common codes for location points and legal entities when communicating via EDI/EDM, EBB/EDM and/or FF/EDM. The corresponding common code name should also be used in EBB/EDM.	RXQ.7.3.21	Trading partners should use common codes for legal entities for the Internet ET 'to' and 'from' data elements.
RXQ.5.3.14	Requests for standardization of additional services and/or data elements should be submitted to the appropriate NAESB quadrant Executive Committee.	4.3.67	A Transportation Service Provider which determines to provide new services which do not utilize existing transaction sets via NAESB WGQ EBB/EDM, should, prior to implementation, submit a request for standardization to NAESB WGQ including descriptions of the EBB/EDM, EDI/EDM and, as applicable, FF/EDM implementation.		DOES NOT EXIST
RXQ.5.3.15	To the extent that multiple EDMs are used (e.g. EDI or Flat-files), the same business result should occur.	4.3.86	To the extent that multiple electronic delivery mechanisms are used, the same business result should occur.		DOES NOT EXIST
RXQ.5.3.16	Non-NAESB Internet ET packages (e.g. PDF files) will have the 'input-format' tag set to 'PAYLOAD' to indicate the format is found in the payload MIME segment. Inside the MIME segment and the 'content-type' header will be set to an appropriate MIME content-type.		DOES NOT EXIST		DOES NOT EXIST

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/Interpretation	ET	Internet ET 2.0
RXQ.5.3.2	All RXQEDM payloads should be encrypted with a minimum 128-bit key when sent on unsecured networks (Internet). This encryption is built into transportation using the NAESB Internet ET. Where other transport options are used, a 128-bit Secure Sockets Layer (SSL) encryption should be used.	4.3.83	For Interactive Flat File EDM, 128-bit Secure Sockets Layer (SSL) encryption should be used.	RXQ.7.3.25	Internet ET Servers should use 128-bit Secure Socket Layer (SSL) encryption.
RXQ.5.3.20	NAESB is a member of ANSI and will strive to remain fully-compliant with ANSI ASC X.12 standards.		DOES NOT EXIST		DOES NOT EXIST
RXQ.5.3.21	RXQ EDI/EDM standards are X.12 compliant.		DOES NOT EXIST		DOES NOT EXIST
RXQ.5.3.22	Where the ANSI ASC X.12 standard does not fully meet a need, NAESB will add interim usages and code values when required. When used, NAESB will submit interim usage/code values to ANSI and the appropriate ANSI organizations for acceptance of the interim solution. ANSI's final solution may provide a usage or code value different from the interim solution. NAESB standards will be updated to reflect the final solution.		DOES NOT EXIST		DOES NOT EXIST

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/Interpretation	ET	Internet ET 2.0
RXQ.5.3.23	EDI Translators generate the ANSI ASC X.12 file, including control numbers and counts that will appear within the ISA/IEA outer envelope segments, and within the GS/GE inner envelope segments.		DOES NOT EXIST		DOES NOT EXIST
RXQ.5.3.24	The ISA is the interchange control segment to be used on all NAESB ANSI ASC X.12 standards.		DOES NOT EXIST		DOES NOT EXIST
RXQ.5.3.25	The Receiver must send a 997 FA for each ANSI ASC X.12 file received.		DOES NOT EXIST		DOES NOT EXIST
RXQ.5.3.26	Inbound EDI transactions should be processed every day business is conducted. The 997 should be sent within one day of business as defined by the Receiver, of the receipt of the ANSI ASC X.12 file.		DOES NOT EXIST		DOES NOT EXIST
RXQ.5.3.27	When Internet ET is used, the Internet ET receipt timestamp is the official receipt timestamp. Without Internet ET, the 997 timestamp is the official receipt timestamp.		DOES NOT EXIST		DOES NOT EXIST
RXQ.5.3.28	RXQEDM uses ANSI ASC X.12 Version 4010 standards unless otherwise noted.		DOES NOT EXIST		DOES NOT EXIST
RXQ.5.3.3	Trading partners should retain transaction data for at least 24	4.3.4	Trading partners should retain transactional data for at least 24	RXQ.7.3.2	Trading partners should retain audit trail

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/Interpretation	ET	Internet ET 2.0
	months for audit purposes. This data retention requirement does not otherwise modify statutory, regulatory, or contractual record retention requirements.		months for audit purposes. This data retention requirement only applies to the ability to recover or regenerate electronic records for a period of two years and does not otherwise modify statutory, regulatory, or contractual record retention requirements.		data for at least 24 months. This data retention requirement does not otherwise modify statutory, regulatory, or contractual record retention requirements.
RXQ.5.3.4	Timestamps that indicate the time transactions were received by a party should be the 'time-c' timestamp from the Internet ET Response.	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 WGQ.	RXQ.7.3.4	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.
RXQ.5.3.40	FF/EDM records are separated by a carriage return/line feed (CRLF or \r\n or ASCII 10 and 13).	4.3.80	NAESB WGQ FF/EDM flat files should be formatted as ASCII comma separated value (CSV) files. This means: Rows are separated by a carriage return/line feed (CRLF). Fields are separated by commas. When a field contains a comma, the field should be enclosed by double-quotes. Double-quotes should not be used within any data field. When numeric data is negative, the minus sign should precede the number. When numeric data contains decimal precision, the decimal point should be included within the field. When numeric data contains one or more		DOES NOT EXIST

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
			significant leading zeros, these zeros should be preserved in the flat file. Date fields should be formatted as YYYYMMDD. Time fields should be specified in a 24 hour format, formatted as HH:MM or HH:MM:SS, as applicable. Date/Time fields should be formatted as YYYYMMDD HH:MM or YYYYMMDD HH:MM:SS when date and time are expressed in one NAESB WGQ data element. Note that there should be exactly one space between the day (DD) and the hour (HH). The maximum amount of data to be placed in a field should be limited to 256 characters. When a field contains no data, the empty field should result in two delimiters next to each other. Note that there should be no blank spaces between the delimiters.		
RXQ.5.3.41	The first record of an FF/EDM Flat-file should be the standard abbreviations for RXQ data elements in the order the corresponding data appears in subsequent rows. The data element order is at the option of the sender.	4.3.81	DOES NOT EXIST		DOES NOT EXIST
RXQ.5.3.42	If an FF/EDM Flat-file data element abbreviation is not recognized, the entire Flat-file should be rejected.	4.3.80	NAESB WGQ FF/EDM flat files should be formatted as ASCII comma separated value (CSV) files. This means: Rows are separated by a carriage return/line feed (CRLF).		DOES NOT EXIST

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
			<p>Fields are separated by commas. When a field contains a comma, the field should be enclosed by double-quotes. Double-quotes should not be used within any data field. When numeric data is negative, the minus sign should precede the number. When numeric data contains decimal precision, the decimal point should be included within the field. When numeric data contains one or more significant leading zeros, these zeros should be preserved in the flat file. Date fields should be formatted as YYYYMMDD. Time fields should be specified in a 24 hour format, formatted as HH:MM or HH:MM:SS, as applicable. Date/Time fields should be formatted as YYYYMMDD HH:MM or YYYYMMDD HH:MM:SS when date and time are expressed in one NAESB WGQ data element. Note that there should be exactly one space between the day (DD) and the hour (HH). The maximum amount of data to be placed in a field should be limited to 256 characters. When a field contains no data, the empty field should result in two delimiters next to each other. Note that there should be no blank spaces between the delimiters.</p>		

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/Interpretation	ET	Internet ET 2.0
RXQ.5.3.43	Each transaction (e.g. Enrollment) should be contained in a single FF/EDM Flat-file record.	4.3.82	For NAESB WGQ FF/EDM flat files, each transaction (e.g. nomination) should be contained in a single row.		DOES NOT EXIST
RXQ.5.3.44	FF/EDM data elements are separated by commas.	4.3.80	<p>NAESB WGQ FF/EDM flat files should be formatted as ASCII comma separated value (CSV) files. This means: Rows are separated by a carriage return/line feed (CRLF). Fields are separated by commas. When a field contains a comma, the field should be enclosed by double-quotes. Double-quotes should not be used within any data field. When numeric data is negative, the minus sign should precede the number. When numeric data contains decimal precision, the decimal point should be included within the field. When numeric data contains one or more significant leading zeros, these zeros should be preserved in the flat file. Date fields should be formatted as YYYYMMDD. Time fields should be specified in a 24 hour format, formatted as HH:MM or HH:MM:SS, as applicable. Date/Time fields should be formatted as YYYYMMDD HH:MM or YYYYMMDD HH:MM:SS when date and time are expressed in one NAESB WGQ data element. Note that there should be exactly one space between the day (DD) and the hour (HH). The</p>		DOES NOT EXIST

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
			maximum amount of data to be placed in a field should be limited to 256 characters. When a field contains no data, the empty field should result in two delimiters next to each other. Note that there should be no blank spaces between the delimiters.		
RXQ.5.3.45	FF/EDM data elements that may contain a comma should be enclosed by double-quotes.	4.3.80	NAESB WGQ FF/EDM flat files should be formatted as ASCII comma separated value (CSV) files. This means: Rows are separated by a carriage return/line feed (CRLF). Fields are separated by commas. When a field contains a comma, the field should be enclosed by double-quotes. Double-quotes should not be used within any data field. When numeric data is negative, the minus sign should precede the number. When numeric data contains decimal precision, the decimal point should be included within the field. When numeric data contains one or more significant leading zeros, these zeros should be preserved in the flat file. Date fields should be formatted as YYYYMMDD. Time fields should be specified in a 24 hour format, formatted as HH:MM or HH:MM:SS, as applicable. Date/Time fields should be formatted as YYYYMMDD HH:MM or YYYYMMDD HH:MM:SS when date and time are expressed in one NAESB		DOES NOT EXIST

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
			WGQ data element. Note that there should be exactly one space between the day (DD) and the hour (HH). The maximum amount of data to be placed in a field should be limited to 256 characters. When a field contains no data, the empty field should result in two delimiters next to each other. Note that there should be no blank spaces between the delimiters.		
RXQ.5.3.46	FF/EDM data elements should not contain double-quotes.	4.3.80	NAESB WGQ FF/EDM flat files should be formatted as ASCII comma separated value (CSV) files. This means: Rows are separated by a carriage return/line feed (CRLF). Fields are separated by commas. When a field contains a comma, the field should be enclosed by double-quotes. Double-quotes should not be used within any data field. When numeric data is negative, the minus sign should precede the number. When numeric data contains decimal precision, the decimal point should be included within the field. When numeric data contains one or more significant leading zeros, these zeros should be preserved in the flat file. Date fields should be formatted as YYYYMMDD. Time fields should be specified in a 24 hour format, formatted as HH:MM or HH:MM:SS, as applicable. Date/Time fields should be		DOES NOT EXIST

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
			formatted as YYYYMMDD HH:MM or YYYYMMDD HH:MM:SS when date and time are expressed in one NAESB WGQ data element. Note that there should be exactly one space between the day (DD) and the hour (HH). The maximum amount of data to be placed in a field should be limited to 256 characters. When a field contains no data, the empty field should result in two delimiters next to each other. Note that there should be no blank spaces between the delimiters.		
RXQ.5.3.47	FF/EDM data elements that contain negative numbers should have the minus sign precede the number.	4.3.80	NAESB WGQ FF/EDM flat files should be formatted as ASCII comma separated value (CSV) files. This means: Rows are separated by a carriage return/line feed (CRLF). Fields are separated by commas. When a field contains a comma, the field should be enclosed by double-quotes. Double-quotes should not be used within any data field. When numeric data is negative, the minus sign should precede the number. When numeric data contains decimal precision, the decimal point should be included within the field. When numeric data contains one or more significant leading zeros, these zeros should be preserved in the flat file. Date fields should be formatted as YYYYMMDD. Time fields should be		DOES NOT EXIST

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
			<p>specified in a 24 hour format, formatted as HH:MM or HH:MM:SS, as applicable. Date/Time fields should be formatted as YYYYMMDD HH:MM or YYYYMMDD HH:MM:SS when date and time are expressed in one NAESB WGQ data element. Note that there should be exactly one space between the day (DD) and the hour (HH). The maximum amount of data to be placed in a field should be limited to 256 characters. When a field contains no data, the empty field should result in two delimiters next to each other. Note that there should be no blank spaces between the delimiters.</p>		
RXQ.5.3.48	FF/EDM data elements that contain decimal precision should include the decimal point within the data element.	4.3.80	<p>NAESB WGQ FF/EDM flat files should be formatted as ASCII comma separated value (CSV) files. This means: Rows are separated by a carriage return/line feed (CRLF). Fields are separated by commas. When a field contains a comma, the field should be enclosed by double-quotes. Double-quotes should not be used within any data field. When numeric data is negative, the minus sign should precede the number. When numeric data contains decimal precision, the decimal point should be included within the field. When numeric data contains one or more significant leading zeros, these zeros</p>		DOES NOT EXIST

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
			<p>should be preserved in the flat file. Date fields should be formatted as YYYYMMDD. Time fields should be specified in a 24 hour format, formatted as HH:MM or HH:MM:SS, as applicable. Date/Time fields should be formatted as YYYYMMDD HH:MM or YYYYMMDD HH:MM:SS when date and time are expressed in one NAESB WGQ data element. Note that there should be exactly one space between the day (DD) and the hour (HH). The maximum amount of data to be placed in a field should be limited to 256 characters. When a field contains no data, the empty field should result in two delimiters next to each other. Note that there should be no blank spaces between the delimiters.</p>		
RXQ.5.3.49	FF/EDM data elements that contain numeric data with one or more significant leading zeros should preserve these zeros within the data element.	4.3.80	<p>NAESB WGQ FF/EDM flat files should be formatted as ASCII comma separated value (CSV) files. This means: Rows are separated by a carriage return/line feed (CRLF). Fields are separated by commas. When a field contains a comma, the field should be enclosed by double-quotes. Double-quotes should not be used within any data field. When numeric data is negative, the minus sign should precede the number. When numeric data contains decimal precision, the decimal point should be</p>		DOES NOT EXIST

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
			<p>included within the field. When numeric data contains one or more significant leading zeros, these zeros should be preserved in the flat file. Date fields should be formatted as YYYYMMDD. Time fields should be specified in a 24 hour format, formatted as HH:MM or HH:MM:SS, as applicable. Date/Time fields should be formatted as YYYYMMDD HH:MM or YYYYMMDD HH:MM:SS when date and time are expressed in one NAESB WGQ data element. Note that there should be exactly one space between the day (DD) and the hour (HH). The maximum amount of data to be placed in a field should be limited to 256 characters. When a field contains no data, the empty field should result in two delimiters next to each other. Note that there should be no blank spaces between the delimiters.</p>		
RXQ.5.3.5	<p>RGQ and REQ require the use of the Internet ET Response 'time-c-qualifier' data element to identify the time-zone of the Receiver's timestamp.</p>	4.3.9	<p>For NAESB WGQ EDI/EDM and FF/EDM, there is a time stamp (HTTP Timestamp) that designates the time that a file is received at the designated site. The receiving party should generate a timestamp upon successful receipt of the complete file and send as an immediate response to the sending party. The timestamp should be generated by Common Gateway Interface (CGI) of the receiving party,</p>	<p>RXQ.7.3.5 and RXQ.7.3.7</p>	<p>A timestamp designates the time a file is received at the Receiver's designated site. The timestamp consists of the 'time-c' data element, and in some cases the 'time-cqualifier' data element. Refer to QEDM standards for</p>

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
			prior to further processing by the CGI. GPD-DOES NOT MATCH		use of the 'time-c-qualifier'. and After timestamp generation, the Receiver and sends an immediate HTTP Response to the Sender. The 'gisb-acknowledgement-receipt', which includes the timestamp data element(s), is the primary part of the HTTP Response.
RXQ.5.3.50	FF/EDM 'date', 'time', and 'date/time' data elements should conform to RXQEDM and ISO standards: date=YYYYMMDD, time=HH:MM:SS, date/time=YYYYMMDD HH:MM:SS	4.3.80	NAESB WGQ FF/EDM flat files should be formatted as ASCII comma separated value (CSV) files. This means: Rows are separated by a carriage return/line feed (CRLF). Fields are separated by commas. When a field contains a comma, the field should be enclosed by double-quotes. Double-quotes should not be used within any data field. When numeric data is negative, the minus sign should precede the number. When numeric data contains decimal precision, the decimal point should be included within the field. When numeric data contains one or more		DOES NOT EXIST

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
			<p>significant leading zeros, these zeros should be preserved in the flat file. Date fields should be formatted as YYYYMMDD. Time fields should be specified in a 24 hour format, formatted as HH:MM or HH:MM:SS, as applicable. Date/Time fields should be formatted as YYYYMMDD HH:MM or YYYYMMDD HH:MM:SS when date and time are expressed in one NAESB WGQ data element. Note that there should be exactly one space between the day (DD) and the hour (HH). The maximum amount of data to be placed in a field should be limited to 256 characters. When a field contains no data, the empty field should result in two delimiters next to each other. Note that there should be no blank spaces between the delimiters.</p>		
RXQ.5.3.51	FF/EDM data elements should be no longer than 256 characters.	4.3.80	<p>NAESB WGQ FF/EDM flat files should be formatted as ASCII comma separated value (CSV) files. This means: Rows are separated by a carriage return/line feed (CRLF). Fields are separated by commas. When a field contains a comma, the field should be enclosed by double-quotes. Double-quotes should not be used within any data field. When numeric data is negative, the minus sign should precede the number. When numeric data contains decimal</p>		DOES NOT EXIST

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
			<p>precision, the decimal point should be included within the field. When numeric data contains one or more significant leading zeros, these zeros should be preserved in the flat file. Date fields should be formatted as YYYYMMDD. Time fields should be specified in a 24 hour format, formatted as HH:MM or HH:MM:SS, as applicable. Date/Time fields should be formatted as YYYYMMDD HH:MM or YYYYMMDD HH:MM:SS when date and time are expressed in one NAESB WGQ data element. Note that there should be exactly one space between the day (DD) and the hour (HH). The maximum amount of data to be placed in a field should be limited to 256 characters. When a field contains no data, the empty field should result in two delimiters next to each other. Note that there should be no blank spaces between the delimiters.</p>		
RXQ.5.3.52	FF/EDM Flat-files should not contain mixed record formats in a single file (e.g. a single file with both Enrollments and Invoices).		DOES NOT EXIST		DOES NOT EXIST
RXQ.5.3.53	FF/EDM payloads should be encrypted prior to Internet transport when not using Internet ET. SSL encryption is sufficient.	4.3.83	For Interactive Flat File EDM, 128-bit Secure Sockets Layer (SSL) encryption should be used.		DOES NOT EXIST

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/Interpretation	ET	Internet ET 2.0
RXQ.5.3.54	Transactions sent using FF/EDM should produce the same business result as other EDMs (e.g. EDI/EDM)	4.3.86	To the extent that multiple electronic delivery mechanisms are used, the same business result should occur.		DOES NOT EXIST
RXQ.5.3.6	Timestamps used within RXQEDM transactions should be generated using clocks that are synchronized with the localized prevailing National Institute of Standards and Technology (NIST) time to mitigate discrepancies between the clocks of the Sender and Receiver. Computer clocks should be synchronized as often as necessary to ensure a +/- 5 second variance with an atomic clock. Specific business processes may have tighter synchronization requirements.	4.3.10	The time-stamp should be included in the HTTP response back to the sender of the original HTTP transaction. The server clock generating the time-stamp 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.	RXQ.7.3.8	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. Computer clocks should be synchronized as necessary to ensure at minimum +/- 5 second synchronization with an atomic clock. Specific business processes may have tighter synchronization requirements.
RXQ.5.3.60	When a party changes the business rule(s) it will apply to documents, it should notify its trading partners at least two weeks in advance of the change(s). The notification should include identification of	4.3.87	4.3.87 When the receiver of: 1) a Nomination, 2) a Pre-determined Allocation, or, 3) a Request for Confirmation, has determined to change the business rule(s) it will apply to the processing of (and/or response to) one or more of these		DOES NOT EXIST

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
	<p>the data element(s) that are changing, the intended business result of such change(s) in the business rule(s), and the scheduled effective date of such change(s).</p>		<p>documents; or, when the sender of: 1) a Confirmation Response (solicited and unsolicited), 2) a Scheduled Quantity, 3) a Scheduled Quantity for Operator, 4) an Allocation, 5) a Shipper Imbalance, or, 6) an Invoice has determined to change the business rule(s) it will apply to the generating of (and/or content within) one or more of these documents, then it should notify its trading partners of same at least two weeks in advance of the change(s). The notification should include identification of the data element(s) that are changing (or whose content is changing), the intended business result of such change(s) in the business rule(s), and the effective date of such change(s). For the purposes of this standard, a business rule change is any change in: a) the presence and/or the acceptable content of a data element which is received by the trading partner sending notice; b) a new business response to an accepted data element which is received by the trading partner sending notice; c) a new business response to the acceptable content of a data element which is received by the trading partner sending notice; or, d) a new intended business result to be communicated to</p>		

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
			<p>a receiver by the trading partner sending notice; Absent mutual agreement between the affected trading partners to the contrary, trading partners notifying their sending or receiving trading partners of a change(s) under this standard should provide the means to test such change(s) during at least a two week time period prior to the effective date of the change(s). Trading partners receiving notice of such change(s) from their trading partner should be prepared not to implement such change(s) even after testing has been completed, as the notifying trading partner is permitted to cancel or postpone such change(s). Notifying trading partners canceling or postponing the effective date of change(s) should provide affected trading partners with notice of cancellation or postponement at least one business day prior to the applicable effective date.</p>		
RXQ.5.3.61	Trading partners implementing Business Rule Changes should provide testing of change(s) during at least a two-week time period prior to the effective date of the change(s).	4.3.87	4.3.87 When the receiver of: 1) a Nomination, 2) a Pre-determined Allocation, or, 3) a Request for Confirmation, has determined to change the business rule(s) it will apply to the processing of (and/or response to) one or more of these documents; or, when the sender of: 1)		DOES NOT EXIST

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
			<p>a Confirmation Response (solicited and unsolicited), 2) a Scheduled Quantity, 3) a Scheduled Quantity for Operator, 4) an Allocation, 5) a Shipper Imbalance, or, 6) an Invoice has determined to change the business rule(s) it will apply to the generating of (and/or content within) one or more of these documents, then it should notify its trading partners of same at least two weeks in advance of the change(s). The notification should include identification of the data element(s) that are changing (or whose content is changing), the intended business result of such change(s) in the business rule(s), and the effective date of such change(s). For the purposes of this standard, a business rule change is any change in:</p> <p>a) the presence and/or the acceptable content of a data element which is received by the trading partner sending notice; b) a new business response to an accepted data element which is received by the trading partner sending notice; c) a new business response to the acceptable content of a data element which is received by the trading partner sending notice; or, d) a new intended business result to be communicated to a receiver by the trading partner</p>		

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
			<p>sending notice; Absent mutual agreement between the affected trading partners to the contrary, trading partners notifying their sending or receiving trading partners of a change(s) under this standard should provide the means to test such change(s) during at least a two week time period prior to the effective date of the change(s). Trading partners receiving notice of such change(s) from their trading partner should be prepared not to implement such change(s) even after testing has been completed, as the notifying trading partner is permitted to cancel or postpone such change(s). Notifying trading partners canceling or postponing the effective date of change(s) should provide affected trading partners with notice of cancellation or postponement at least one business day prior to the applicable effective date.</p>		
RXQ.5.3.62	<p>Trading partners are permitted to cancel or postpone scheduled changes. Notice of cancellation or postponement should be provided to trading partners at least one business day prior to the scheduled effective date.</p>	4.3.87	<p>4.3.87 When the receiver of: 1) a Nomination, 2) a Pre-determined Allocation, or, 3) a Request for Confirmation, has determined to change the business rule(s) it will apply to the processing of (and/or response to) one or more of these documents; or, when the sender of: 1) a Confirmation Response (solicited</p>		DOES NOT EXIST

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
			<p>and unsolicited), 2) a Scheduled Quantity, 3) a Scheduled Quantity for Operator, 4) an Allocation, 5) a Shipper Imbalance, or, 6) an Invoice has determined to change the business rule(s) it will apply to the generating of (and/or content within) one or more of these documents, then it should notify its trading partners of same at least two weeks in advance of the change(s). The notification should include identification of the data element(s) that are changing (or whose content is changing), the intended business result of such change(s) in the business rule(s), and the effective date of such change(s). For the purposes of this standard, a business rule change is any change in:</p> <p>a) the presence and/or the acceptable content of a data element which is received by the trading partner sending notice; b) a new business response to an accepted data element which is received by the trading partner sending notice; c) a new business response to the acceptable content of a data element which is received by the trading partner sending notice; or, d) a new intended business result to be communicated to a receiver by the trading partner sending notice; Absent mutual</p>		

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
			agreement between the affected trading partners to the contrary, trading partners notifying their sending or receiving trading partners of a change(s) under this standard should provide the means to test such change(s) during at least a two week time period prior to the effective date of the change(s). Trading partners receiving notice of such change(s) from their trading partner should be prepared not to implement such change(s) even after testing has been completed, as the notifying trading partner is permitted to cancel or postpone such change(s). Notifying trading partners canceling or postponing the effective date of change(s) should provide affected trading partners with notice of cancellation or postponement at least one business day prior to the applicable effective date.		
RXQ.5.3.63	Trading partners should use dedicated testing systems that are representative of production systems.		DOES NOT EXIST		DOES NOT EXIST
RXQ.5.3.7	When Internet ET is used, the Internet ET Receipt timestamp supercedes any EDM timestamps with respect to official time the document was received by the Receiver.	[11].3.2 7	When Internet ET is used, the Internet ET receipt timestamp is the official receipt timestamp. Without Internet ET, the 997 timestamp is the official receipt timestamp.		DOES NOT EXIST

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/Interpretation	ET	Internet ET 2.0
RXQ.5.3.8	When Internet ET is not used, the receipt timestamp is defined by each specific EDM.		DOES NOT EXIST		DOES NOT EXIST
RXQ.5.3.9	RXQEDM 'date' data elements should be formatted as YYYYMMDD.	4.3.80	<p>NAESB WGQ FF/EDM flat files should be formatted as ASCII comma separated value (CSV) files. This means: Rows are separated by a carriage return/line feed (CRLF). Fields are separated by commas. When a field contains a comma, the field should be enclosed by double-quotes. Double-quotes should not be used within any data field. When numeric data is negative, the minus sign should precede the number. When numeric data contains decimal precision, the decimal point should be included within the field. When numeric data contains one or more significant leading zeros, these zeros should be preserved in the flat file. Date fields should be formatted as YYYYMMDD. Time fields should be specified in a 24 hour format, formatted as HH:MM or HH:MM:SS, as applicable. Date/Time fields should be formatted as YYYYMMDD HH:MM or YYYYMMDD HH:MM:SS when date and time are expressed in one NAESB WGQ data element. Note that there should be exactly one space between the day (DD) and the hour (HH). The maximum amount of data to be placed</p>		DOES NOT EXIST

RxQ	RxQ Model Business Practices/Definitions/Principles/Interpretations	WGQ	WGQ 1.7 Original Standards/Definitions/Principal/ Interpretation	ET	Internet ET 2.0
			in a field should be limited to 256 characters. When a field contains no data, the empty field should result in two delimiters next to each other. Note that there should be no blank spaces between the delimiters.		

FOR EVALUATION PURPOSES ONLY

Contracts

The following contracts, model agreements, and outlines have been developed for retail use:

RXQ.6.1	Electronic Data Interchange Trading Partner Agreement	Page 124
RXQ.6.2	Outline of a Non-Disclosure Agreement	Page 125
RGQ.6.3	Distribution Supplier Service Agreement Outline	Page 131
REQ.6.3	Distribution Supplier Service Agreement Outline	Page 140
RXQ.6.4	Billing Services Agreement Outline For Consolidated Billing	Page 149

RXQ.6.1 Electronic Data Interchange Trading Partner Agreement

The Electronic Data Interchange Trading Partner Agreement (EDI TPA) and the NAESB Trading Partner Agreement User's Guide for Use in Retail Applications are included in Appendix 1 to this book so that the format of the model contract is not modified. An executable version of the EDI TPA is downloadable from the NAESB web site (<http://www.naesb.org>).

FOR EVALUATION PURPOSES ONLY

RXQ.6.2 Outline of a Non-Disclosure Agreement

The following outline for a non-disclosure agreement (“Agreement”) attempts to address the issues surrounding information considered to be confidential which must be shared between two parties. This outline provides a framework from which to create a specific non-disclosure agreement and is not intended to be a formal, legal document.

FOR EVALUATION PURPOSES ONLY

TABLE OF CONTENTS

1 GENERAL AND ADMINISTRATIVE PROVISIONS

1.1 Purpose of Agreement

1.2 Term of Agreement

1.3 Actions to be Taken Upon Termination of Agreement

1.4 Assignment

2 TYPES OF INFORMATION CONSIDERED CONFIDENTIAL

3 USAGE AND PROTECTIONS OF INFORMATION CONSIDERED CONFIDENTIAL

4 DISCLOSURE OF INFORMATION CONSIDERED CONFIDENTIAL

5 ENFORCEABILITY

6 REMEDIES

7 REPRESENTATIONS AND WARRANTIES

8 CONTACT INFORMATION

9 DISCLAIMERS

10 MISCELLANEOUS PROVISIONS

11 SIGNATURES

1 GENERAL AND ADMINISTRATIVE PROVISIONS

The opening section typically names the parties to which the Agreement applies and the date on which the Agreement was initially signed.

1.1 Purpose of Agreement

This section identifies in general terms the purpose of the Agreement and the general terms and conditions that bind the parties, either during the initial contact with a potential business partner or after a business relationship has been established.

Typical clauses may include the following:

- a. Neither party is obligated under this Agreement to purchase from or provide to the other party any service or product.
- b. There are other applicable laws, regulations, codes, etc. that govern the relationship.

1.2 Term of Agreement

This section defines the effective date of the Agreement (which may differ from the date on which it is signed) and the date the Agreement will terminate. This section also includes a description of the process by which one party may inform the other of its desire to terminate the Agreement.

The date of termination may coincide with any of the following:

- a. The date that a modified or new Agreement commences;
- b. The date that certain automatic termination clauses come into effect.

1.3 Actions to be taken Upon Termination of Agreement

This section describes the actions to be taken by either party upon termination of the Agreement (e.g. return or destruction of information considered confidential), including the timing of such actions.

This section also states what protections would continue after the termination of the Agreement.

1.4 Assignment

This section defines the terms and conditions under which a party to the Agreement may assign its rights or obligations to a third party.

Typically, clauses would say that neither party may assign its rights or obligations hereunder, except to an affiliate or successor in interest, without the prior written consent of the other party, which consent shall not be unreasonably withheld.

2 TYPES OF INFORMATION CONSIDERED CONFIDENTIAL

This section defines the types of information considered confidential as covered by the Agreement. Such information may vary depending upon the nature of the specific Non-Disclosure Agreement.

This section also defines when the protections afforded by this Agreement may not apply to certain information.

Typically, protections may not apply to information that:

- a. Was publicly known at the time of the party's communication of this information to the receiving party;
- b. Becomes publicly known through no fault of the receiving party or affiliate subsequent to the time of the party's communication of this information to the receiving party;
- c. Was rightfully in the receiving party's or affiliate's possession free from any obligation of confidence at the time of the party's communication of this information to the receiving party;
- d. Is rightfully obtained by the receiving party or affiliate from third parties authorized to make such disclosure without restriction;
- e. Is identified by the party's communication to no longer be proprietary or confidential; or
- f. Is required to be disclosed by existing laws, regulations, or court orders.

3 USAGE AND PROTECTIONS OF INFORMATION CONSIDERED CONFIDENTIAL

This section describes the specific usage of the information considered confidential as defined in the Agreement.

For example, if this is an Agreement for creditworthiness, this section could limit the usage of such information by the Creditor for the purpose of evaluation of the financial status of the Applicant and/or the Applicant's affiliates as it relates to a determination by the Creditor of whether or not the parties may enter into a written contract for the supply or delivery of energy.

The section also describes the protections of the information considered confidential.

For example, typical protections might be that the party receiving the information shall protect such information from disclosure to others, using the same degree of care used to protect its own confidential or proprietary information of like importance (i.e. physical or electronic access), but in any case using no less than a reasonable degree of care.

This section also defines who owns the information considered confidential.

4 DISCLOSURE OF INFORMATION CONSIDERED CONFIDENTIAL

This section lists the conditions under which and to whom the information considered to be confidential may be disclosed.

a. The party receiving the information could, for example, be limited to disclosing such information to affiliates, employees, agents, etc. based on those who have a need to know and are bound to protect the received information from unauthorized use and disclosure under the terms of the Agreement.

b. In the event a party is required by law, regulation or court order to disclose any of the information, the party will promptly notify the other party prior to making any such disclosure.

5 ENFORCEABILITY

This section describes the law and forum applicable to the Agreement.

This section also describes the enforceability of the Agreement under certain conditions.

For example, if any provision of this Agreement is found to be unenforceable, the remainder shall be enforced as fully as possible and the unenforceable provision shall be deemed modified to the limited extent required to permit its enforcement in a manner most closely representing the intention of the parties expressed herein.

This section typically contains a statement that any delay or omission in enforcing any terms of the Agreement shall not be deemed a waiver of the right to enforce such terms and that any waiver of a breach of the Agreement shall not constitute a waiver as to any future breach.

6 REMEDIES

This section describes the remedies available to the parties in the event either party fails to comply with the provisions of the Agreement (e.g. injunctive relief, damages).

7 REPRESENTATIONS AND WARRANTIES

This section describes any representations and warranties provided.

8 CONTACT INFORMATION

This section typically provides the name, address, telephone number, facsimile number, and e-mail address of the primary and alternate designated contacts for each party.

9 DISCLAIMERS

This section typically lists disclaimers regarding items such as the responsibility for costs and the nature of the relationship.

This section may also disclaim accuracy, completeness, etc., of the information considered confidential as well as disclaiming liability resulting from the use of the information considered confidential.

10 MISCELLANEOUS PROVISIONS

This section typically includes a statement that neither party shall be paid a fee for entering into this Agreement.

This section also typically includes a statement that this Agreement does not preclude the parties from collecting any additional costs as directed or authorized by a legislative body, administrative body, or court having jurisdiction over such issues.

This section may also include a statement as to the whether and under what circumstances the existence of this Agreement may be made public.

This section may include a statement that this Agreement constitutes the entire agreement between the parties and may be modified only in writing as mutually agreed to by the parties.

11 SIGNATURES

This section includes the names and signatures of the signatories to the Agreement for each party.

This section may also include a certification statement that says the signatory is duly authorized to sign for the party

RGQ.6.3 Distribution Supplier Service Agreement Outline

The following outline for a “Distribution Company - Supplier Service Agreement” (“Agreement”) attempts to provide a framework in which to create a jurisdiction-specific Agreement consistent with the jurisdiction’s Governing Documents. The outline is not intended to be a formal, legal document that dictates the terms and conditions of the contractual relationship between the Distribution Company and Supplier. Each jurisdiction has its own set of Governing Documents that may or may not address the details of a contractual relationship between Distribution Companies and Suppliers. Thus, terms of the ultimate Agreement will reflect the structure of the individual retail market.

TABLE OF CONTENTS

Introduction	X
1 GENERAL AND ADMINISTRATIVE PROVISIONS	X
1.1 Purpose of Agreement	X
1.2 Definitions	X
1.3 Term of Agreement	X
1.4 Amendments and Modifications to Agreement	X
1.5 Assignment, Delegation and Subcontracting	X
1.6 Third Party Beneficiaries	X
1.7 Enforceability	X
1.8 Notices	X
1.9 Relevant Documents	X
1.10 Waivers	X
2 CONDITIONS PRECEDENT	X
3 EVENTS OF DEFAULT AND REMEDIES FOR DEFAULT	X
4 LIMITATION OF LIABILITY	X
5 INDEMNIFICATION	X
6 FORCE MAJEURE	X
7 SYSTEM OPERATION	X
8 SECURITY ARRANGEMENTS	X
9 METERING	X
10 UNAUTHORIZED ENERGY USE	X
11 CUSTOMER BILLING AND PAYMENTS	X
12 BILLING AND PAYMENTS BETWEEN MARKET PARTICIPANTS	X
13 COMMUNICATION PROCESS	X
14 CUSTOMER INQUIRIES	X
15 AUDITS	X
16 DISPUTE RESOLUTION PROCESS	X
17 NONDISCLOSURE/CONFIDENTIALITY	X
18 REPRESENTATIONS AND WARRANTIES	X
19 MISCELLANEOUS PROVISIONS	X
19.1 Survival	X
19.2 Non-Waiver	X
19.3 Entire Agreement	X
19.4 Taxes	X
20 CONTACT INFORMATION	X
21 SIGNATURES	X

1 GENERAL AND ADMINISTRATIVE PROVISIONS

The opening section typically names the parties to which the Distribution Company-Supplier Service Agreement (the Agreement) applies and the date on which the Agreement was signed.

1.1 Purpose of Agreement

This section identifies, in general terms, the purpose of the document and the general terms and conditions that bind the parties. Typical clauses may include the following:

- a. This is a legally binding agreement governing the business relationship between the parties as it pertains to gas supply, metering services, billing, etc.
- b. This agreement is not to be interpreted as a joint venture arrangement.
- c. There are other applicable laws, regulations, codes, etc. that govern the relationship.

1.2 Definitions

This section may be included to define terms that are relevant to the Agreement.

1.3 Term of Agreement

This section defines the effective date of the Agreement and the date the Agreement will terminate. The date of termination may coincide with any of the following:

- a. Notification by a Supplier that no longer wishes to operate in a Distribution Company's service territory;
- b. The date that a modified or new service agreement commences; or
- c. The date that certain automatic termination clauses come into effect, such as those described in the "Event of Default" section.

This section may also include a description of the process by which one party may inform the other of its intent to terminate the Agreement.

1.4 Amendments and Modifications to Agreement

This section identifies the rules for amending or modifying the Agreement.

1.5 Assignment, Delegation and Subcontracting

This section defines the terms and conditions under which a party to the Agreement may assign its rights or obligations to a third party. Typically, clauses would say that neither party may assign rights or obligations without the prior written consent of the non-assigning party. Such clauses usually distinguish between assignment and subcontracting. Subcontracting is not an assignment of rights or obligations, but rather a means of fulfilling the rights and obligations of the contracting party through a subcontractor. Subcontracting provisions may also say that neither party may utilize subcontractors without the prior written consent of the

non-subcontracting party.

1.6 Third Party Beneficiaries

This section reiterates the parties that are subject to this Agreement and states that there are no third-party beneficiaries.

1.7 Enforceability

This section describes the enforceability of the Agreement under certain conditions. For example:

- a. Severability: If any provision of this Agreement or application thereof is held invalid or unenforceable, the remainder of the provisions in this Agreement shall not be affected and shall continue in full force, unless deletion of the provision results in the failure of the Agreement to address its central purpose.
- b. Governing law: This section identifies the applicable venue under which the Agreement will be enforced (e.g., state and federal laws).
- c. Effect of headings: This section states that headings and subheadings have no effect on interpretation of terms of the Agreement.

1.8 Notices

This section indicates that all notices under the Agreement shall be in writing and acknowledges the rights of parties to change the contact persons' name and address to which notices should be sent. Any special requirements with respect to delivery options may be delineated here. Reference may be made to the contact persons and addresses listed in an appendix.

1.9 Relevant Documents

This section may reference other applicable tariffs, laws, regulations, codes, regulatory guidelines, rules, operational manuals, etc., which govern or affect the relationship.

In the event of a conflict, conditions and requirements in certain Governing Documents may take precedence over the terms and conditions in the Agreement. This section also should describe the hierarchy of documents (i.e., which document takes precedence in the event of a conflict).

Most jurisdictions promulgate detailed rules by which the competitive gas retail market and retail market participants must operate. These rules tend to be described in documents separate from a contractual agreement (e.g., legislation, codes, regulatory guidelines). These rules may include processes in which a Distribution Company and Supplier may interact. For example:

- a. Retail settlements/reconciliation
- b. Customer information
- c. Customer switching

- d. Load obligations of the Supplier
- e. Load profiles used by the Distribution Company
- f. Utilization of schedule coordinators and agreements
- g. System operations/curtailment
- h. Delivery and balancing
- i. Tariffs and fees

Details on these processes could be included in this Agreement by reference, or actually detailed in the Agreement itself. If these rules are incorporated by reference, a summary of the relevant documents could be included here or in an appendix. Alternatively, each of the above topics could be developed as separate sections. To the extent the operating conditions are not spelled out in other documents, these conditions may need to be addressed specifically in the text of the Agreement.

1.10 Waivers

Although an agreement usually is subject to the legislative and regulatory requirements of the jurisdiction, this section may be included to define any waivers of conditions in the relevant documents.

2 CONDITIONS PRECEDENT

This section would include a list of the conditions that must be in place prior to entering into the Agreement or prior to either the Agreement becoming effective or to commencing service under the Agreement. Examples may include:

- a. Each party is licensed as required under applicable laws and regulations.
- b. Each party is in compliance with applicable laws, regulations, license conditions, market rules, etc.
- c. The parties have satisfied all applicable creditworthiness requirements.
- d. The Supplier has entered into the appropriate agreements with schedule coordinators to allow the Supplier to serve load.
- e. The requisite electronic funds transfer arrangements are in place.

This section may note that these conditions precedent are ongoing obligations of the parties and failure to continue to meet these conditions may provide grounds for default or eventual termination of the Agreement.

3 EVENTS OF DEFAULT AND REMEDIES FOR DEFAULT

This section defines the conditions under which a Supplier or Distribution Company would be considered in default of the Agreement. Examples may include:

- a. Non-payment

- b. Bankruptcy
- c. Violation of license conditions or regulations, including Customer slamming
- d. Non-compliance with terms and conditions of the Agreement, including security arrangements or conditions precedent

This section describes the actions that either party may or must take when a default occurs. Such remedies may be prescribed by applicable regulatory requirements or by general commercial law. This section may also include statements concerning the ongoing obligations of each party. Examples of remedies include the following:

- a. Description of notification requirements
- b. Period of time during which a party can correct the default before termination of the Agreement

Specific remedies associated with particular events may be described in the relevant sections of the Agreement.

This section may specify the interest rate that would be paid by the defaulting party during periods of default. Any other arrangements made by the parties to remedy defaults may also be included.

4 LIMITATION OF LIABILITY

This section defines the extent of liability of each party. Liability is often limited to direct or actual damages incurred as a result of a party's action, lack of action, default, or wrongful termination. Typically, damages such as consequential, indirect, special, or punitive are specifically excluded by this section.

5 INDEMNIFICATION

This section typically provides that each party shall hold harmless the other party from claims by a third party due to the negligence of the indemnifying party, subject to the limitations of liability. For example, in the event that the Distribution Company is authorized to physically disconnect the Customer on behalf of the Supplier, the Agreement should indemnify the Distribution Company against any damages resulting from that action. Indemnification typically extends beyond the termination of the Agreement.

6 FORCE MAJEURE

This section relieves the parties of liability due to events beyond their control. Such events are defined in this section.

A description of the process by which a party informs the other of the event of force majeure may also be included.

7 SYSTEM OPERATION

This section may be included to delineate the rights of the Distribution Company to physically disconnect, curtail, interrupt or reduce service to Customers and/or require Suppliers to adjust the schedule or delivery of its supplies whenever the Distribution

Company reasonably determines that such an act is necessary to maintain system reliability, or is directed to do so by an appropriate third party, such as a regional transmission authority, government agency, or civil authority. Notifications to Market Participants and related issues may also be included.

8 SECURITY ARRANGEMENTS

This section delineates in general terms the requisite creditworthiness requirements of the parties and describes any potential security arrangements that may be established between the parties, or refers to other Governing Documents that specify creditworthiness requirements.

9 METERING

Where applicable, this section describes the conditions under which a Market Participant may provide competitive metering services. This section may also include a reference to any metering requirements stated in other Governing Documents.

If metering services are not unbundled, this section would describe the metering options made available to a Supplier by the Distribution Company.

10 UNAUTHORIZED ENERGY USE

This section may be included to incorporate specific provisions, protections and penalties related to unauthorized energy use by the end use Customer. It also could be used to create an obligation on both parties to inform the other if unauthorized energy use is suspected.

11 CUSTOMER BILLING AND PAYMENTS

This section delineates, in general terms, the standard billing and payment arrangements that may be established between the parties, or refers to other Governing Documents that specify billing and payment requirements (e.g. a Billing Services Agreement).

12 BILLING AND PAYMENTS BETWEEN MARKET PARTICIPANTS

This section delineates, in general terms, the standard billing and payment arrangements that may be established between the parties, or refers to other Governing Documents that specify billing and payment requirements between the parties.

13 COMMUNICATION PROCESS

This section describes the communication process by which required reports, data, and information are communicated between parties.

14 CUSTOMER INQUIRIES

If applicable, this section describes the process by which each party is obligated to handle Customer inquiries. This may include decision rules on which calls (if any) one party might handle for the other and the preferred method for getting the Customer in touch with the correct party (live transfer, referral, etc.).

15 AUDITS

This section identifies the rights of each party and the circumstances under which one party has the right to audit the other party's transactions and procedures that directly relate to the conditions of the Agreement. This section may also specify the time frame and other potential limitations on the right to audit.

16 DISPUTE RESOLUTION PROCESS

This section describes the dispute resolution process established between the parties, or refers to other Governing Documents that specify the dispute resolution process requirements.

17 NONDISCLOSURE/CONFIDENTIALITY

This section defines the type of information that is considered confidential and the responsibility of each party to maintain the confidentiality of such information, or refers to other Governing Documents that specify the parties' requirements for maintaining confidentiality. This section may also specify remedies for breaching the confidentiality requirements.

18 REPRESENTATIONS AND WARRANTIES

This section describes any representations and warranties provided.

19 MISCELLANEOUS PROVISIONS

19.1 Survival

This section states that certain obligations, such as confidentiality, payment of money due, warranties, remedies, and indemnity for events arising prior to termination or expiration, survive expiration or termination of the Agreement.

19.2 Non-Waiver

This section provides that a party's failure to insist on strict performance of any provision of the Agreement is not construed as a waiver of its right to enforce the provision in the future.

19.3 Entire Agreement

This section includes a declaration that:

- a. This Agreement contains the entire agreement of the parties;
- b. There are no other oral or written agreements between the parties on this subject matter that aren't reflected in this Agreement, and;
- c. This Agreement supersedes prior agreements.

19.4 Taxes

This section contains a provision that specifies responsibility for collection and payment of any applicable taxes.

20 CONTACT INFORMATION

This section typically provides the name, address, telephone number, facsimile number, and e-mail address of the primary and alternate designated contacts for each party.

21 SIGNATURES

This section includes the printed name, title, signature, and date for all signatories to the Agreement for each party.

This section may also include a certification statement that indicates the signatories are duly authorized to sign for the parties.

FOR EVALUATION PURPOSES ONLY

REQ.6.3 Distribution Supplier Service Agreement Outline

The following outline for a “Distribution Company - Supplier Service Agreement” (“Agreement”) attempts to provide a framework in which to create a jurisdiction-specific Agreement consistent with the jurisdiction’s Governing Documents. The outline is not intended to be a formal, legal document that dictates the terms and conditions of the contractual relationship between the Distribution Company and Supplier. Each jurisdiction has its own set of Governing Documents that may or may not address the details of a contractual relationship between Distribution Companies and Suppliers. Thus, terms of the ultimate Agreement will reflect the structure of the individual retail market.

FOR EVALUATION PURPOSES ONLY

TABLE OF CONTENTS

Introduction		X
1	GENERAL AND ADMINISTRATIVE PROVISIONS	X
1.1	Purpose of Agreement	X
1.2	Definitions	X
1.3	Term of Agreement	X
1.4	Amendments and Modifications to Agreement	X
1.5	Assignment, Delegation and Subcontracting	X
1.6	Third Party Beneficiaries	X
1.7	Enforceability	X
1.8	Notices	X
1.9	Relevant Documents	X
1.10	Waivers	X
2	CONDITIONS PRECEDENT	X
3	EVENTS OF DEFAULT AND REMEDIES FOR DEFAULT	X
4	LIMITATION OF LIABILITY	X
5	INDEMNIFICATION	X
6	FORCE MAJEURE	X
7	SYSTEM OPERATION	X
8	SECURITY ARRANGEMENTS	X
9	METERING	X
10	UNAUTHORIZED ENERGY USE	X
11	CUSTOMER BILLING AND PAYMENTS	X
12	BILLING AND PAYMENTS BETWEEN MARKET PARTICIPANTS	X
13	COMMUNICATION PROCESS	X
14	CUSTOMER INQUIRIES	X
15	AUDITS	X
16	DISPUTE RESOLUTION PROCESS	X
17	NONDISCLOSURE/CONFIDENTIALITY	X
18	REPRESENTATIONS AND WARRANTIES	X
19	MISCELLANEOUS PROVISIONS	X
19.1	Survival	X
19.2	Non-Waiver	X
19.3	Entire Agreement	X
19.4	Taxes	X
20	CONTACT INFORMATION	X
21	SIGNATURES	X

1 GENERAL AND ADMINISTRATIVE PROVISIONS

The opening section typically names the parties to which the Distribution Company-Supplier Service Agreement (the Agreement) applies and the date on which the Agreement was signed.

1.1 Purpose of Agreement

This section identifies, in general terms, the purpose of the document and the general terms and conditions that bind the parties. Typical clauses may include the following:

- a. This is a legally binding agreement governing the business relationship between the parties as it pertains to electricity supply, metering services, billing, etc.
- b. This agreement is not to be interpreted as a joint venture arrangement.
- c. There are other applicable laws, regulations, codes, etc. that govern the relationship.

1.2 Definitions

This section may be included to define terms that are relevant to the Agreement.

1.3 Term of Agreement

This section defines the effective date of the Agreement and the date the Agreement will terminate. The date of termination may coincide with any of the following:

- a. Notification by a Supplier that no longer wishes to operate in a Distribution Company's service territory;
- b. The date that a modified or new service agreement commences; or
- c. The date that certain automatic termination clauses come into effect, such as those described in the "Event of Default" section.

This section may also include a description of the process by which one party may inform the other of its intent to terminate the Agreement.

1.4 Amendments and Modifications to Agreement

This section identifies the rules for amending or modifying the Agreement.

1.5 Assignment, Delegation and Subcontracting

This section defines the terms and conditions under which a party to the Agreement may assign its rights or obligations to a third party. Typically, clauses would say that neither party may assign rights or obligations without the prior written consent of the non-assigning party. Such clauses usually distinguish between assignment and subcontracting. Subcontracting is not an assignment of rights or obligations, but rather a means of fulfilling the rights and

obligations of the contracting party through a subcontractor. Subcontracting provisions may also say that neither party may utilize subcontractors without the prior written consent of the non-subcontracting party.

1.6 Third Party Beneficiaries

This section reiterates the parties that are subject to this Agreement and states that there are no third-party beneficiaries.

1.7 Enforceability

This section describes the enforceability of the Agreement under certain conditions. For example:

- a. Severability: If any provision of this Agreement or application thereof is held invalid or unenforceable, the remainder of the provisions in this Agreement shall not be affected and shall continue in full force, unless deletion of the provision results in the failure of the Agreement to address its central purpose.
- b. Governing law: This section identifies the applicable venue under which the Agreement will be enforced (e.g., state and federal laws).
- c. Effect of headings: This section states that headings and subheadings have no effect on interpretation of terms of the Agreement.

1.8 Notices

This section indicates that all notices under the Agreement shall be in writing and acknowledges the rights of parties to change the contact persons' name and address to which notices should be sent. Any special requirements with respect to delivery options may be delineated here. Reference may be made to the contact persons and addresses listed in an appendix.

1.9 Relevant Documents

This section may reference other applicable tariffs, laws, regulations, codes, regulatory guidelines, rules, operational manuals, etc., which govern or affect the relationship.

In the event of a conflict, conditions and requirements in certain Governing Documents may take precedence over the terms and conditions in the Agreement. This section also should describe the hierarchy of documents (i.e., which document takes precedence in the event of a conflict).

Most jurisdictions promulgate detailed rules by which the competitive electricity retail market and retail market participants must operate. These rules tend to be described in documents separate from a contractual agreement (e.g., legislation, codes, regulatory guidelines). These rules may include processes in which a Distribution Company and Supplier may interact. For example:

- a. Retail settlements/reconciliation
- b. Customer information

- c. Customer switching
- d. Load obligations of the Supplier
- e. Load profiles used by the Distribution Company
- f. Utilization of schedule coordinators and agreements
- g. System operations/curtailment
- h. Delivery and balancing
- i. Tariffs and fees

Details on these processes could be included in this Agreement by reference, or actually detailed in the Agreement itself. If these rules are incorporated by reference, a summary of the relevant documents could be included here or in an appendix. Alternatively, each of the above topics could be developed as separate sections. To the extent the operating conditions are not spelled out in other documents, these conditions may need to be addressed specifically in the text of the Agreement.

1.10 Waivers

Although an agreement usually is subject to the legislative and regulatory requirements of the jurisdiction, this section may be included to define any waivers of conditions in the relevant documents.

2 CONDITIONS PRECEDENT

This section would include a list of the conditions that must be in place prior to entering into the Agreement or prior to either the Agreement becoming effective or to commencing service under the Agreement. Examples may include:

- a. Each party is licensed as required under applicable laws and regulations.
- b. Each party is in compliance with applicable laws, regulations, license conditions, market rules, etc.
- c. The parties have satisfied all applicable creditworthiness requirements.
- d. The Supplier has entered into the appropriate agreements with schedule coordinators to allow the Supplier to serve load.
- e. The requisite electronic funds transfer arrangements are in place.

This section may note these conditions precedent are ongoing obligations of the parties and failure to continue to meet these conditions may provide grounds for default or eventual termination of the Agreement.

3 EVENTS OF DEFAULT AND REMEDIES FOR DEFAULT

This section defines the conditions under which a Supplier or Distribution Company would be considered in default of the Agreement. Examples may include:

- a. Non-payment
- b. Bankruptcy
- c. Violation of license conditions or regulations, including Customer slamming
- d. Non-compliance with terms and conditions of the Agreement, including security arrangements or conditions precedent

This section describes the actions that either party may or must take when a default occurs. Such remedies may be prescribed by applicable regulatory requirements or by general commercial law. This section may also include statements concerning the ongoing obligations of each party. Examples of remedies include the following:

- a. Description of notification requirements
- b. Period of time during which a party can correct the default before termination of the Agreement

Specific remedies associated with particular events may be described in the relevant sections of the Agreement.

This section may specify the interest rate that would be paid by the defaulting party during periods of default. Any other arrangements made by the parties to remedy defaults may also be included.

4 LIMITATION OF LIABILITY

This section defines the extent of liability of each party. Liability is often limited to direct or actual damages incurred as a result of a party's action, lack of action, default, or wrongful termination. Typically, damages such as consequential, indirect, special, or punitive are specifically excluded by this section.

5 INDEMNIFICATION

This section typically provides that each party shall hold harmless the other party from claims by a third party due to the negligence of the indemnifying party, subject to the limitations of liability. For example, in the event that the Distribution Company is authorized to physically disconnect the Customer on behalf of the Supplier, the Agreement should indemnify the Distribution Company against any damages resulting from that action. Indemnification typically extends beyond the termination of the Agreement.

6 FORCE MAJEURE

This section relieves the parties of liability due to events beyond their control. Such events are defined in this section.

A description of the process by which a party informs the other of the event of force majeure may also be included.

7 SYSTEM OPERATION

This section may be included to delineate the rights of the Distribution Company to physically disconnect, curtail, interrupt or reduce service to Customers whenever the Distribution Company reasonably determines that such an act is necessary to maintain system reliability, or is directed to do so by an appropriate third party, such as a regional transmission authority, government agency, or civil authority. Notifications to Market Participants and related issues may also be included.

8 SECURITY ARRANGEMENTS

This section delineates in general terms the requisite creditworthiness requirements of the parties and describes any potential security arrangements that may be established between the parties, or refers to other Governing Documents that specify creditworthiness requirements.

9 METERING

Where applicable, this section describes the conditions under which a Market Participant may provide competitive metering services. This section may also include a reference to any metering requirements stated in other Governing Documents.

If metering services are not unbundled, this section would describe the metering options made available to a Supplier by the Distribution Company.

10 UNAUTHORIZED ENERGY USE

This section may be included to incorporate specific provisions, protections and penalties related to unauthorized energy use by the end use Customer. It also could be used to create an obligation on both parties to inform the other if unauthorized energy use is suspected.

11 CUSTOMER BILLING AND PAYMENTS

This section delineates, in general terms, the standard billing and payment arrangements that may be established between the parties, or refers to other Governing Documents that specify billing and payment requirements (e.g. a Billing Services Agreement).

12 BILLING AND PAYMENTS BETWEEN MARKET PARTICIPANTS

This section delineates, in general terms, the standard billing and payment arrangements that may be established between the parties, or refers to other Governing Documents that specify billing and payment requirements between the parties.

13 COMMUNICATION PROCESS

This section describes the communication process by which required reports, data, and information are communicated between parties.

14 CUSTOMER INQUIRIES

If applicable, this section describes the process by which each party is obligated to handle Customer inquiries. This may include decision rules on which calls (if any) one party might handle for the other and the preferred method for getting the Customer in touch with the correct party (live transfer, referral, etc.).

15 AUDITS

This section identifies the rights of each party and the circumstances under which one party has the right to audit the other party's transactions and procedures that directly relate to the conditions of the Agreement. This section may also specify the time frame and other potential limitations on the right to audit.

16 DISPUTE RESOLUTION PROCESS

This section describes the dispute resolution process established between the parties, or refers to other Governing Documents that specify the dispute resolution process requirements.

17 NONDISCLOSURE/CONFIDENTIALITY

This section defines the type of information that is considered confidential and the responsibility of each party to maintain the confidentiality of such information, or refers to other Governing Documents that specify the parties' requirements for maintaining confidentiality. This section may also specify remedies for breaching the confidentiality requirements.

18 REPRESENTATIONS AND WARRANTIES

This section describes any representations and warranties provided.

19 MISCELLANEOUS PROVISIONS

19.1 Survival

This section states that certain obligations, such as confidentiality, payment of money due, warranties, remedies, and indemnity for events arising prior to termination or expiration, survive expiration or termination of the Agreement.

19.2 Non-Waiver

This section provides that a party's failure to insist on strict performance of any provision of the Agreement is not construed as a waiver of its right to enforce the provision in the future.

19.3 Entire Agreement

This section includes a declaration that:

- a. This Agreement contains the entire agreement of the parties;
- b. There are no other oral or written agreements between the parties on this subject matter that aren't reflected in this Agreement, and;
- c. This Agreement supersedes prior agreements.

19.4 Taxes

This section contains a provision that specifies responsibility for collection and payment of any applicable taxes.

20 CONTACT INFORMATION

This section typically provides the name, address, telephone number, facsimile number, and e-mail address of the primary and alternate designated contacts for each party.

21 SIGNATURES

This section includes the printed name, title, signature, and date for all signatories to the Agreement for each party.

This section may also include a certification statement that indicates the signatories are duly authorized to sign for the parties.

RXQ.6.4 Billing Services Agreement For Consolidated Billing

This Billing Services Agreement outline provides market participants with a framework from which to create a jurisdiction specific agreement based on structure, rules and Governing Documents of the jurisdiction. This outline is not intended to be a formal, legal document that dictates the terms and conditions of the contractual relationship between the Distribution Company and the Supplier where one is the Billing Party and the other is the Non-Billing Party. Terms of the executed Billing Services Agreement will be legally binding on the parties and will reflect the structure of a particular retail market.

FOR EVALUATION PURPOSES ONLY

BILLING SERVICES AGREEMENT OUTLINE FOR CONSOLIDATED BILLING

PREFACE

General description of the Billing Services Agreement.

Scope and relationships with other Governing Documents.

Identification of the parties to the Billing Services Agreement.

Effective date and term of the Billing Services Agreement.

Conditions precedent to the execution of the Billing Services Agreement (e.g. data exchange protocols, licensing, creditworthiness, and billing system capability).

KEY COMPONENTS

Identification of Billing Party [Supplier or Distribution Company].

Identification of the Consolidated Billing option(s) [Bill Ready and / or Rate Ready].

Type of payment processing option(s) selected by the Billing Party [Assumption of Receivables or Pay As You Get Paid].

Definition of terms used in the Billing Services Agreement.

BILLING OBLIGATIONS AND OPTIONS

Specify relevant responsibilities, terms and conditions between the parties for the Consolidated Billing option(s) selected including: performance parameters, financial arrangements, and other details (e.g. bill format, bill insert requirements, timing for receiving Non-Billing Party charges, lead time for price changes, responsibility for calculating late payment charges, fees for billing services, accuracy of Non-Billing Party charges).

Specify any creditworthiness criteria that the Non-Billing Party's Customers would have to satisfy to be eligible for Consolidated Billing.

Specify responsibilities for non-standard billing arrangements to be provided to the Non-Billing Party by the Billing Party for selected Customers (e.g., issue bills on non-standard cycle, non-standard pricing).

Specify responsibilities for non-energy charges (e.g., billing for energy management services).

Specify responsibilities for billing features that affect both parties (e.g., budget billing).

Specify responsibilities for the usage cancellation or re-statement process.

Specify responsibilities for the bill cancellation and re-bill process.

PAYMENT OBLIGATIONS AND OPTIONS

Specify responsibilities, terms and conditions for payments due to the Non-Billing Party from the Billing Party related to their Consolidated Billing of Customers, including performance parameters, financial arrangements, creditworthiness, notification of Customer bills In Dispute, and other details (e.g., method of payment, timing of payment, payment advice timing, payment posting order).

Specify responsibilities, terms and conditions for payments due to the Billing Party from the Non-Billing Party related to their Consolidated Billing of Customers including fees for billing services (e.g., method of payment, timing of payment, charges for late payments).

Specify the level of discount (to include uncollectibles, arrearages, and the time value of money, etc.) to be reflected in the amount due for Assumption of Receivables method, if applicable.

Specify the conditions to change the level of uncollectibles to be reflected in the amount due for Assumption of Receivables method, is applicable.

Specify responsibilities, terms and conditions when the Billing Party provides payment arrangements to a Customer on behalf of the Non-Billing Party (e.g., terms for payment by the Customers in arrears).

COLLECTION OBLIGATIONS AND OPTIONS

Specify activities related to the collection actions to be taken by each party (e.g., collection of late payment charges, Customer notification).

Specify responsibilities, terms and conditions for the Billing Party to carry forward arrears on a Customer's account no longer served by the Non-Billing Party (e.g., Billing Party will carry charges for the Non-Billing Party on the bill for a specified period of time, returning outstanding arrears to the Non-Billing Party).

Specify the threshold for overdue payments and identified delinquencies that can result in the conversion of a Customer to Dual Billing or to regulated energy supply service (e.g., timing of conversion).

Specify the terms and conditions a customer must satisfy to be eligible for return to Consolidated Billing.

When the Distribution Company is not the Billing Party, specify the responsibilities, terms and conditions for providing the Distribution Company with access to real-time Billing Party payment information for specific Customer accounts in order for the Distribution Company to take appropriate collection action.

Identify special handling arrangements for collection of funds for specific Customer accounts.

Specify the terms and conditions regarding customer dispute resolution practices.

SERVICE LEVEL AND REMEDIES

Specify expectations for performance and responsibilities of each party, including remedies for failure to meet obligations (e.g., Non-Billing Party calls for change due to Billing Party performance).

Specify terms and conditions for the Billing Party to pay interest to the Non-Billing Party when payment for undisputed charges is not made to the Non-Billing Party within the appropriate time frame.

Specify terms and conditions for the Non-Billing Party to pay interest to the Billing Party when payment for billing services rendered is not made to the Billing Party within the appropriate time frame.

Specify the provisions for reviewing and auditing Billing Party activities on behalf of the Non-Billing Party.

Specify the terms of the Non-Billing Party's payment for billing services rendered by the Billing Party on behalf of the Non-Billing Party (e.g., timing and method of payment).

INTERNET ELECTRONIC TRANSPORT

Executive Summary

The North American Energy Standards Board (NAESB) Wholesale Gas Quadrant (WGQ), Retail Electric Quadrant (REQ), and Retail Gas Quadrant (RGQ) have developed standards for electronic commerce over the Internet. The Internet Electronic Transport (Internet ET) standards enable the rapid, reliable, and safe transportation of electronic information between NAESB trading partners.

This document is a high-level guide to implementing various technologies necessary to communicate transactions and other electronic data using standard protocols. As such, this guide is not intended to be a comprehensive, in-depth manual. Where possible, this guide points to more in-depth material. The Reference section provides locations on the Internet to obtain more information as well as recommended books and periodicals.

Parties should refer to market Governing Documents for specific implementations of Internet ET.

Business Reasons for Using Internet ET

Energy companies need to exchange information and data with other energy companies. Internet ET enables this with the following advantages:

Security. Internet ET incorporates the PAIN security principles of Privacy, Authenticity, Integrity and Non-repudiation.

Standardized Process. Internet ET standardizes how packages are exchanged, regardless of the business process, the trading partner, or the energy quadrant.

Audit Trail. Internet ET gives both Sender and Receiver a detailed audit trail, enabling better controls and less errors.

Error Notification. Internet ET prescribes how errors are to be handled, and provides a foundation for efficient and quick resolution to errors.

Minimum technology requirements. Internet ET is built on low-cost technology and readily-available Web browser and open source technology.

Interactive and Batch Capabilities. Internet ET provides mechanisms for both fully-automated and manual-assisted business processes.

Any Payloads. Internet ET can deliver any kind of payload, whether it is EDI, flat-files, XML, documents, etc.

Software Standards. The Internet ET standards increase the likelihood that software vendors will provide Commercial Off-The-Shelf (COTS) software packages.

Overview of Electronic Transport Life Cycle

In the Internet ET life-cycle, the party sending data, the 'Sender', creates an electronic package by encrypting the data payload and applying appropriate header 'envelope' information such as 'to' and 'from'. This electronic package is submitted to the trading partner's SSL Web server as an HTTP Request using the POST

method.

The receiving party, the ‘Receiver’, receives and decrypts the package, then forwards the payload data to back-office processes. A Receipt is sent from the Receiver to the Sender with timestamps and any error notices. The Receiver back-office systems process the data according to NAESB quadrant-specific Electronic Delivery Mechanisms (QEDM), quadrant-specific standards (e.g. ‘Nominations’), Trading Partner Agreements, and related documents. If the Receiver decrypts in a separate process, the Receiver may send an Error Notification package to the Sender to identify errors found during decryption.

Trading partners can be either the Sender or Receiver depending on what information and data needs to be exchanged.

The Internet ET standards focus on the transport of the electronic package and not the contents of the package. Each business process may define different contents, and the Internet ET is designed to work with any type of contents (e.g. EDI, flat files, etc).

The following are Internet ET life-cycle scenarios:

1. **Success.** The Successful scenario is when the electronic package was delivered with no errors, and the Sender has received a Receipt from the Receiver.
2. **Invalid Package Response.** The Invalid Package Response scenario is when the Receiver was unable to disassemble the electronic package, and has sent an HTTP Response to the Sender notifying them of package errors.
3. **Invalid Package Error Notification.** The Invalid Package Error Notification scenario is when a Receiver detects an error in the package AFTER the Response is sent. This scenario exists when a Receiver has implemented processes where the decryption occurs after the Response is sent. Decryption errors are communicated to the Sender via an HTTP Request using the Internet ET Error Notification format.
4. **Exchange Failure.** The Exchange Failure scenario is when a Sender is unable to establish and/or maintain a connection with the Server to send an electronic package to the Receiver.

Errors detected after successful decryption (e.g. format errors, EDI errors, etc) are beyond the scope of the Internet ET, and can be found in the QEDM standards.

Parties implementing Internet ET should become familiar with the following components of the Internet ET:

- Internet ET Network and Communications Requirements
- Sending Internet ET Electronic Packages
- Receiving Internet ET Electronic Packages
- Security

Key Assumptions

This document makes the following assumptions:

- **Platform Independence.** An Internet ET implementation can communicate with all trading partners in the energy industry, regardless what hardware, operating system and programming languages trading partners use.
- **Open Standards.** NAESB has adopted open standard technologies to provide flexibility and scalability.
- **Payload Content Independence.** Internet ET standards focus on the transport of the electronic package, and not the contents of the package. Each business process may define different contents. Internet ET is designed to work with any type of content (e.g. EDI, flat files, etc). The Internet ET's main function is to get the package from point X to point Y reliably with privacy, authentication, integrity, and non-repudiation.
- **Importance of the Technical Exchange Worksheet (TEW).** Internet ET relies on the exchange of technical information between trading partners to establish and maintain reliable Internet ET production. This worksheet is intended to establish communications between two parties. Additional requirements and information may be required. Refer to your quadrant-specific EDM (QEDM). A sample TEW is included in Appendix C. The TEW may be a part of a Trading Partner Agreement (TPA).
- **Testing With Internet ET Trading Partners.** Since the Internet ET is not platform-specific, testing with other trading partners on a variety of platforms is very important in ensuring that each Internet ET application is compatible with a range of platforms used by various trading partners. Testing should ensure receipt of the package, proper decryption, and appropriate Receipts were sent.
- **Business Process Considerations.** Implementers of business processes that use Internet ET should be aware of the following issues that may impact business process design:

The Internet Lacks Quality of Service (QoS). The Internet is unable to assign priority to file transfers. High-priority NAESB Internet ET package transfers such as Nominations have no priority over low-priority Internet transfers such as music MP3 files or other lower-priority NAESB Internet ET transfers. Business processes that have firm or tight Internet ET transfer timing requirements should be constructed to properly mitigate the risk associated with this lack of guaranteed QoS on the Internet. QoS may be improved by using a private network in lieu of the Internet.

Clock Synchronization. The Internet ET allows +/- 5 seconds variance from an NIST atomic clock. Business processes with more stringent requirements may need to implement more restrictive synchronization requirements and processes.

Exchange Failures. When trading partners systems are failing, parties are required to attempt to send Internet ET packages 3 times over a minimum period of 30-minutes before notifying trading partners of exchange failures. Business processes with more stringent requirements may need to implement more restrictive exchange failure requirements and processes.

- **Examples Provided in this Document.** The examples provided in this document are for illustration only. Implementers should rely on the standards and not on these examples when implementing the Internet ET.

FOR EVALUATION PURPOSES ONLY

Introduction

The North American Energy Standards Board (NAESB) is a voluntary non-profit organization comprised of members from all aspects of the greater gas and electric industries.

NAESB Internet Electronic Transport (Internet ET) Standards are used by the Wholesale Gas Quadrant (WGQ), Retail Electric Quadrant (REQ), and the Retail Gas Quadrant (RGQ) for the electronic transport of transactions and other information payloads between trading partners.

NAESB recognizes that as the energy industry evolves and uses NAESB standards, additional and amended NAESB standards will be necessary. Any industry participant seeking additional or amended standards (including principles, definitions, standards, data elements, process descriptions, technical implementation instructions) should submit a request detailing the change to the NAESB office so that the appropriate process may take place to amend the standards.

Business Processes and Practices

RXQ.7 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 2.0 of the Internet ET standard incorporates all electronic transport technical specifications of the NAESB WGQ EDM Version 1.7.

Roles in Internet ET

In the Internet ET life-cycle, one party sends a package, and the other party receives the package. The party sending the package is referred to as the Sender or Client, and the party receiving the package is also referred to as the Receiver or Server.

NAESB business processes often require that parties act in both the Sender and Receiver roles. For example, once the Receiver of a payload file of Nominations has successfully processed the payload, they switch to the Sender role to send Nomination acknowledgements back to the original Sender. Internet ET implementations may need to implement both Sender and Receiver capabilities.

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.

To establish an Internet ET trading partnership with another company, a company needs to exchange technical information about their Internet ET implementation. This may include:

- Contact information
- Public Keys, including key exchange and update policies
- Test URLs
- Production URLs, including alternative paths if available
- Common Code Identifiers (e.g. DUNS number)
- Use of 'time-c-qualifier' if in REQ or RGQ

This may be exchanged using a Technical Exchange Worksheet (TEW). A sample TEW is in Appendix C. In some cases, this information may be exchanged with a Trading Partner Agreement.

Implementation Approaches

The NAESB Internet ET can be constructed using any IT deployment model, including the use of in-house development, consulting/development help from a third-party, Commercial Off-The-Shelf (COTS) software, or 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 unauthorized parties.

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.

Internet ET Network and Communication Requirements

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.
- 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
---	-----	---

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

In this context redundancy refers to normal operations redundancy, not to disaster recovery contingencies. Disaster recovery contingencies are not addressed in NAESB Internet ET standards.

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.

TCP Communications

NAESB Internet ET Principle 4.1.x37 and NAESB Internet ET Standard 4.3.x70 restrict the TCP ports used as a standard for Internet ET communications. The use of NAESB standard TCP ports may require modifications in the Sender's and Receiver's firewalls to allow for communications with various trading partners' Internet ET implementations. Parties should indicate to their trading partners which specific TCP ports are required to be opened to conduct electronic communication.

Internet ET allows the following TCP Ports (not UDP ports)

- HTTP HTTPS 80, 443, 5713, 6112, 6304, 6874, 7403
- TCP Optional 8001-8020**

**The reservation of 20 optional ports provides for additional security and for implementations such as load balancing. Parties should minimize the number of ports used for Internet ET.

Other Communication Protocols

HTTP POST - HTTP POST is the standard method for transporting Internet ET packages to trading partners. The POST method allows the upload of complete datasets without special encoding.

MIME 'multi-part' - Internet ET packages are created using the 'multi-part' content type.

Sending Internet ET Packages

Internet ET supports both interactive and batch browsers. Interactive web browsers provide for low-cost access to Internet ET capabilities. 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 trading partners in real-time or near real-time, while providing better audit trails.

Receiving Internet ET Packages

Receiving Internet ET packages and transaction payloads requires 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 timestamp for the package
- Stores the payload file
- Sends the Receipt as an HTTP Response to the Sender/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, often referred to by the acronym PAIN, are vital to protecting Internet ET packages:

- **D**ata **P**rivacy
- **A**uthentication
- **D**ata **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:

OpenPGP, defined by (IETF RFC 2440) with modifications described in this specification	OR	PGP 2.6 or higher, with RSA keys can be used on a mutually agreed basis
--	-----------	---

Internet ET uses base64-encoding and 128-bit SSL to protect username and password.

Authentication

Authentication is the assurance to one entity that another entity is who he/she/it claims to be. Basic authentication is the required standard to prevent intruders from connecting to Internet ET Web sites. Internet ET uses 128-bit SSL-protected usernames and passwords to establish authentication. Optional 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 OpenPGP/PGP 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 may optionally include 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.

RXQ.7.1 Principles

- RXQ.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 energy transactions.
- RXQ.0.1.2** 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.
- RXQ.7.1.1** The Internet Electronic Transport (ET) does not pick winners, rather it should create an environment where the marketplace can dictate a winner or winners.
- RXQ.7.1.2** Internet ET solutions should be cost effective, simple and economical.
- RXQ.7.1.3** Internet ET solutions should provide for a seamless marketplace for energy.
- RXQ.7.1.4** Parties should interface with third-party vendors according to NAESB Internet ET standards.
- RXQ.7.1.5** 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.
- RXQ.7.1.6** Protocols and tools that parties elect to support should be 'Internet-compatible'.
- RXQ.7.1.7** The NAESB Internet ET should not set standards for site-level security. Individual organization security standards should be relied upon.
- RXQ.7.1.8** 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.
- RXQ.7.1.9** 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.

RXQ.7.2 Definitions

- RXQ.0.2.56 'Internet ET Testing'**. Testing electronic packages between trading partners includes testing of: A) Connectivity; B) Encryption/Decryption; and C) Digital signatures where

appropriate.

- RXQ.0.2.57 'Fail-over'** defines a prescribed process executed when a NAESB Internet ET Client fails to establish a connection to the target NAESB Internet ET Server.
- RXQ.0.2.58 'Trading Partner'** is a party that enters into an agreement with another party to transact business electronically using the Internet ET standard.
- RXQ.0.2.59 'Originating party'** is any party originating/creating the package. This could also include a third-party.
- RXQ.0.2.60 'Third-Party'** is any organization that a trading party uses to provide services to comply with the required elements of the Internet ET.
- RXQ.0.2.61 'Receiving Party'** is any party that hosts (either in-house or outsourced) an Internet ET compliant server capable of receiving Internet ET packages.
- RXQ.0.2.62 'Receiving Program'** is a program or set of programs that process HTTP Requests from a Sender. The Receiving Program is responsible for generating the 'gisb-acknowledge-receipt', which includes any party that hosts (either in-house or outsourced) an Internet ET compliant server capable of receiving Internet ET packages.
- RXQ.0.2.63 'Trading Partner Agreement', or 'TPA'** is a legal agreement between trading parties. The TPA often dictates service level agreements and problem remediation processes. The TPA may include technical exchange information such as URLs, et cetera.
- RXQ.0.2.64 'Batch Browser'**. A Browser that can be run with little or no manual operation or intervention. See 'Browser'.
- RXQ.0.2.65 'Browser'**. A software program capable of generating HTTP Requests, including HTTP POST requests.
- RXQ.0.2.66 'Client'**. The computer hardware and software used by the Sender to transmit an Electronic Package to the Receiver's Server. A Client can be fully-automated or manual.
- RXQ.0.2.67 'COTS'**. Commercial Off-The-Shelf; software that can be purchased and that requires little or no customization.
- RXQ.0.2.68 'Electronic Package'**. A data stream sent via HTTP POST that contains envelope header information and Payload File(s). The Payload Files are encrypted using defined Internet ET encryption techniques.
- RXQ.0.2.69 'Error Notification'**. Error Notification is a package sent from the Receiver of the original data to the Sender when errors are trapped after the Internet ET Receipt is sent. This is normally

used for decryption errors detected after the Internet ET Receipt has been sent.

- RXQ.0.2.70 'HTTP Request'**. The stream of data sent from the Client to the Server that includes header information and payload data.
- RXQ.0.2.71 'HTTP Response'**. The stream of data sent from the Server to the Client in response to an HTTP Request, including the Receipt.
- RXQ.0.2.72 'HTTP Server'**. The computer hardware and software used by the Receiver to receive HTTP Requests from the Sender's Client, and to send HTTP Responses to the Sender's Client. The Server is an HTTP/Web Server.
- RXQ.0.2.73 'IETF'**. Internet Engineering Task Force; a body of technical experts that set standards for the Internet known as Request for Comments (RFC's).
- RXQ.0.2.74 'Interactive Browser'**. A Browser that requires manual operation or intervention. See 'Browser'.
- RXQ.0.2.75 'Internet EDM'**. The GISB and NAESB WGQ standards up to and including Version 1.7. The 'Internet ET' and 'QEDM' standards were derived from these WGQ EDM standards.
- RXQ.0.2.76 'Internet ET' or 'Internet Electronic Transport'**. The NAESB standards for the secure transport of electronic information between trading partners, building upon WGQ EDM Version 1.7.
- RXQ.0.2.77 'Payload Files'**. The data contents inside of an electronic package. NAESB Internet ET is content-independent.
- RXQ.0.2.78 'Protocol Failure'**. A protocol failure occurs any time a sending party's NAESB Internet ET server cannot connect to the receiving party's NAESB Internet ET server. For example, if a server tries to connect to a server and fails, or tries to post a file and fails, this is a protocol failure.
- RXQ.0.2.79 'Exchange Failure'**. An exchange failure is when a sending party's NAESB Internet ET server has had three or more protocol failures over a period of time no less than thirty minutes and no more than two hours.
- RXQ.0.2.80 'QEDM'**. Quadrant-specific Electronic Delivery Mechanism; the set of standards for each NAESB quadrant that define the EDM standards for EDI, flat-files, electronic bulletin boards, and other technologies. The QEDM excludes electronic transport practices and standards. The QEDMs were derived from the GISB and NAESB WGQ Internet EDM standards.
- RXQ.0.2.81 'Receipt'**. The HTTP Response sent from the Receiver to the Sender that includes the 'gisb-acknowledge-receipt' section with

a timestamp and OK/error status.

RXQ.0.2.82 ‘Receiver’. The party that receives an Internet ET electronic package.

RXQ.0.2.83 ‘Sender’. The party that sends an Electronic Package.

RXQ.0.2.84 ‘QoS’. Quality of Service; term used to define what level of network bandwidth is guaranteed or assured. The Internet does not offer guaranteed quality of service.

RXQ.0.2.85 ‘Technical Exchange Worksheet’ or ‘TEW’. A document or worksheet used to communicate important information related to the technical implementation of Internet ET; includes information such as URLs, contacts and Public Key policies.

RXQ.0.2.86 ‘TCP’. Transmission Control Protocol; IETF RFCs 793, 1122, 1323

See <http://www.itprc.com/tcpipfaq/default.htm>.

RXQ.0.2.87 ‘RSA’. A mathematical algorithm for encryption developed by Rivest/Shamir/Adleman.

See <http://world.std.com/~fran/crypto/rsa-guts.html>.

RXQ.0.2.88 ‘SSL’. Secure Sockets Layer; a privacy technique that uses encryption to hide information from electronic observers on the Internet. See

<http://developer.netscape.com/docs/manuals/security/sslin/contents.htm>.

RXQ.0.2.89 ‘PGP’. Pretty Good Privacy; software used to create Public and Private Keys for privacy and digital signature applications. See <http://www.uk.pgp.net/pgpnet/pgp-faq/>

RXQ.0.2.90 ‘Private Key’. The sequence of digits known as a ‘key’ that is kept private by the owner of a digital certificate, and is used by the certificate owner in encryption and decryption algorithms.

RXQ.0.2.91 ‘Public Key’. The sequence of digits known as a ‘key’ that an owner of a digital certificate shares with trading partners. The trading partners use the public key in encryption and decryption algorithms in electronic transactions with the certificate owner.

RXQ.0.2.92 ‘HTTP’. Hypertext transport protocol; Assumes version HTTP/1.1; IETF RFCs 2616, 2069.

See <http://www.w3.org/Protocols/Specs.html>.

RXQ.0.2.93 ‘MIME’. Multipurpose Internet Mail Extensions; IETF RFCs 2045, 2046, 2047, 2048, 2049;

See <http://www.faqs.org/rfcs/rfc2045.html>.

RXQ.7.3 Standards:

RXQ.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:

when contracting party provides a D-U-N-S® Number at the Branch Location level;

OR

to accommodate accounting for an entity that is identified at the Branch Location level.

RXQ.7.3.1 All parties sending and receiving data should accept a TCP/IP connection.

RXQ.7.3.2 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.

RXQ.7.3.3 The designated Internet ET Server/Receiver site should be accessible via the public Internet. This does not preclude location of the designated site on a private intranet, as long as the designated site is also accessible via the public Internet.

RXQ.7.3.4 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.

RXQ.7.3.5 A timestamp designates the time a file is received at the Receiver’s designated site. The timestamp consists of the ‘time-c’ data element, and in some cases the ‘time-c-qualifier’ data element. Refer to QEDM standards for use of the ‘time-c-qualifier’.

RXQ.7.3.6 The Receiver generates a timestamp upon the successful receipt of a complete file. The timestamp should be generated by the Receiving Program immediately, prior to further processing by the Receiving Program.

RXQ.7.3.7 After timestamp generation, the Receiver sends an immediate HTTP Response to the Sender. The ‘gisb-acknowledgement-receipt’, which includes the timestamp data element(s), is the primary part of the HTTP Response.

RXQ.7.3.8 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. Computer clocks should be synchronized as necessary to ensure at minimum +/- 5 second synchronization with an atomic clock.

Specific business processes may have tighter synchronization requirements.

RXQ.7.3.9 The HTTP Response should be sent to the Internet Protocol (IP) address of the HTTP Request.

RXQ.7.3.10 At a minimum, 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.

RXQ.7.3.11 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 (IETF RFC 1945).

RXQ.7.3.12 A failure to complete a unit of work is a protocol failure.

RXQ.7.3.13 Three protocol failures within a 30-minute timeframe is an exchange failure.

RXQ.7.3.14 The Internet ET roles for 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 HTTP Request	Read HTTP Request	Start of Receipt
Write HTTP Request	Read HTTP Request	
EOF (send)	Read HTTP Request	End of Receipt
Read HTTP Response Received	Write HTTP Response	
EOF HTTP Response		

RXQ.7.3.15 Trading partners should implement all security features (privacy, secure authentication, integrity, and non-repudiation) using a file-based approach via a commercially-available implementation of:

- An OpenPGP product as defined by IETF RFC 2440, or
- On a mutually agreed basis, PGP version 2.6 or greater using the RSA algorithm to generate keys

RXQ.7.3.16 Trading partners should implement basic authentication.

RXQ.7.3.17 Encryption keys should be self-certified. The exchange of Public keys should be completed electronically such as via email. The exchange of Private keys, if applicable, should be done in a secure manner such as via postal or courier mail. Key policies, including key exchange policies should be communicated to trading partners.

- RXQ.7.3.18** 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.
- RXQ.7.3.19** Internet protocols should be used for accessing all industry business functions.
- RXQ.7.3.20** Batch and Interactive Browsers should use Internet-compatible common browser software.
- RXQ.7.3.21** Trading partners should use common codes for legal entities for the Internet ET 'to' and 'from' data elements.
- RXQ.7.3.22** Private network connections to NAESB Internet ET servers, which include all NAESB 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.
- RXQ.7.3.23** Parties should be limited to the NAESB Internet ET approved list of available TCP ports for Internet ET implementations.
- RXQ.7.3.24** Internet ET implementations should not require any inbound ports to be opened on the Sender's firewall.
- RXQ.7.3.25** Internet ET Servers should use 128-bit Secure Socket Layer (SSL) encryption.

D. Interpretations

NAESB has adopted the following interpretations of WGQ standards that relate to Internet ET implementation.

- 7.3.50** The question is whether individual implementations are free to use HTTP HEAD command, prior to using the POST command to deliver the NAESB payload. When implementing a NAESB Internet ET solution, the standard clearly relies on the HTTP protocol spec for details of how to implement the protocol. It is also clear that the HTTP POST command should be used, and not the GET command.

Interpretation:

The use of the HTTP HEAD command in NAESB Internet ET is an option, and as such its implementation between trading partners is solely on a 'mutually agreed to' basis, i.e. the Requester is free to propose the use of the HEAD command to its trading partners, but the Requester cannot insist upon its use. Moreover, the Requester must still provide for transmission and receipt, via the standards, to those trading partners that do not consent to the use of the HEAD

command. If the Requester seeks the use of the HEAD command as an explicit requirement of NAESB Internet ET they are directed to submit a Request for Standard to NAESB.

Related Standards

COMMON CODES

Internet ET uses the D-U-N-S® Number as the common company identifier for the HTTP Request and Response data dictionary 'to' and 'from' HTTP header elements. The D-U-N-S® Number is a 9-digit number assigned to companies by the Dun & Bradstreet Corporation (D&B). The D-U-N-S+4® Number is a 10- to 13-digit number, where characters 10 through 13 are arbitrarily assigned by the owner of the D-U-N-S® Number.

For Internet ET Common Code purposes, an entity will use one and only one D-U-N-S® Number. Entity common codes should be 'legal entities,' that is, Ultimate Location, Headquarters Location, and/or Single Location (in D&B terms). However, in the following situations, a Branch Location (in D&B terms) can also be an entity common code:

1. When the contracting party provides a D-U-N-S® Number at the Branch Location level.
2. To accommodate accounting for an entity that is identified at the Branch Location level.

Since D&B offers customers the option of carrying more than one D-U-N-S® Number per entity, please refer to NAESB's Web Page at www.naesb.org for directions on determining the one and only one D-U-N-S® Number constituting the NAESB Internet ET Entity Common Code.

QUADRANT-SPECIFIC ELECTRONIC DELIVERY MECHANISMS (QEDM)

In NAESB business processes, the Internet ET standards are used in conjunction with Quadrant-Specific Electronic Delivery Mechanism standards, found in the QEDM book for each Quadrant. These standards include, but are not limited to, X12/EDI standards, flat-file standards, web standards, etc.

PARTY ROLES

Various types of parties are involved in NAESB business processes and the use of Internet ET, including distribution companies, end-users, regulatory entities, service providers, and suppliers.

Technical Implementation - INTERNET ET

INTERNET ET TECHNOLOGIES

The NAESB Internet ET uses the following technologies and components to securely and reliably transport electronic packages to trading partners:

- OpenPGP and PGP encryption and digital signatures
- TCP/IP and HTTP POST. Internet ET uses a specifically-structured HTTP POST to transport payload data from one trading partner to the other
- MIME multi-part encoding. Internet ET package structure requires that each section of the package be encoded
- A 'Client', running at the Sender's site as 'batch' or 'interactive' browser software. This software is referred to in this document as 'Client'
- A 'Server' running at the Receiver's site, usually on a dedicated computer. This is a Web or HTTP server, and is referred to in this document as 'Server'

ELECTRONIC TRANSPORT LIFE CYCLE

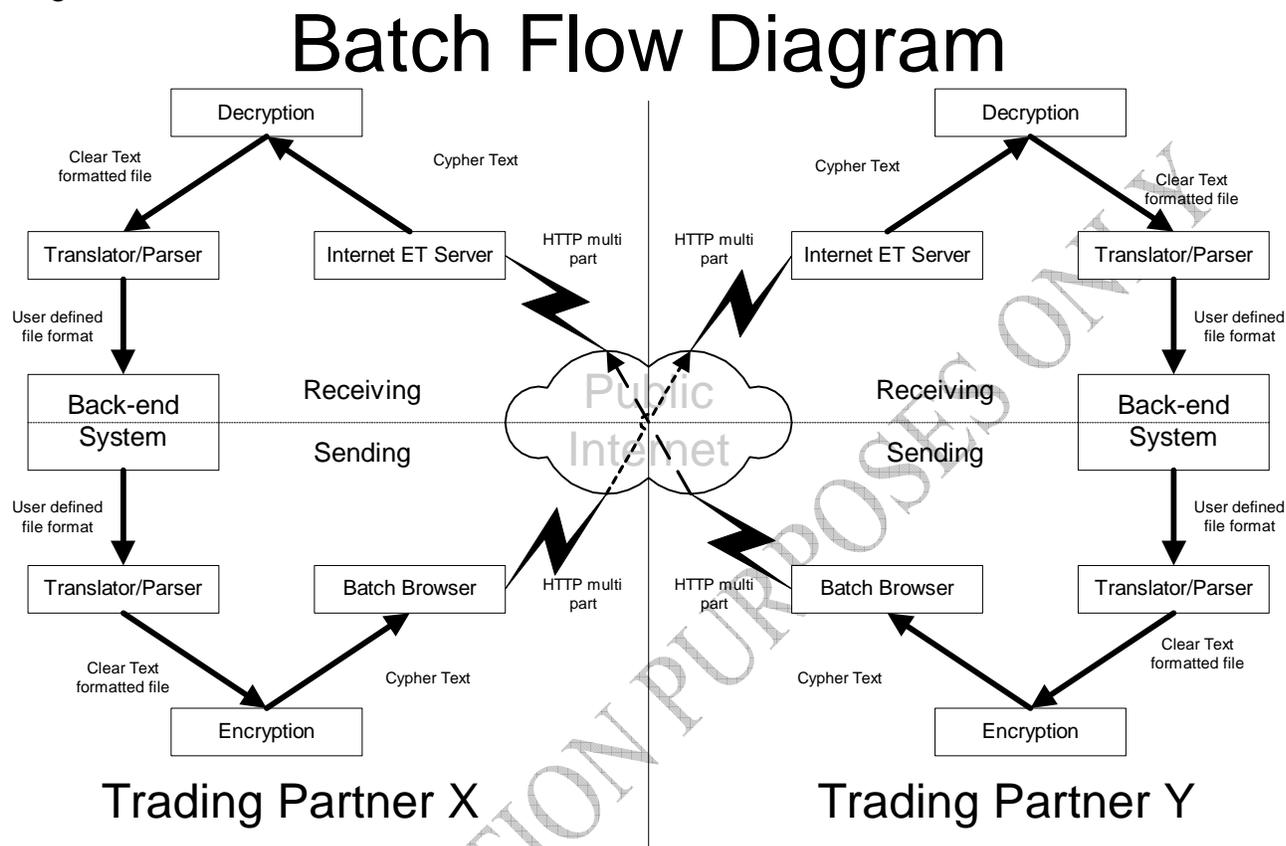
The life cycle of an Electronic Package using Internet ET is described below:

• Sender		• Receiver
<ul style="list-style-type: none"> • Collects payload data to be sent • Encrypts payload • Prepares digital signature if necessary 		
<ul style="list-style-type: none"> • Uses browser to create Electronic Package multi-part HTTP Request with header data elements and payload. • Uses HTTP POST to send the electronic package to the Receiver 	↓	
		<ul style="list-style-type: none"> • Receives the HTTP Request on their Web/HTTP Server • Validates Sender information from HTTP Request Header data elements and payload • **Decrypts payload file • Prepares Receipt • Checks digital signatures if necessary
	↙	<ul style="list-style-type: none"> • Sends Receipt with either 'OK' or error message
<ul style="list-style-type: none"> • Updates logs • If errors, correct errors then repeat process 		<ul style="list-style-type: none"> • **Decrypts payload file
	↙	<ul style="list-style-type: none"> • If errors in decryption, sends Error Notification to Sender
<ul style="list-style-type: none"> • Receives Error Notification • Updates logs • correct errors then repeat process 		<ul style="list-style-type: none"> • Updates logs • If no errors, Receiver processes contents of payload

**Parties may choose to decrypt file before or after Receipt is sent to Sender.

Batch Flow Diagram

The flow of data to and from trading partners in an automated environment is diagrammed below.



ANATOMY OF AN INTERNET ET PACKAGE

An Internet ET package consists of the following sections:

- **Envelope header.** This section contains the envelope information needed to communicate who the Sender and Receiver are, as well as other envelope information.
- **Payload.** This section contains the payload file. Internet ET allows for only one payload file per package.
- **Digital Signatures.** If used, the package should contain a section that is the digital signature.

ENVELOPE DATA DICTIONARY

The data dictionary on the next page details standard data elements, each with element name and description.

Data Dictionary for Internet ET

Business Name	Definition	Format	Usage*	Condition
from**	the party sending the transaction	Common Code Identifier format	in Request; M	used in file transmittal; displayed in HTTP Response; and, used in posting back decryption-related errors
input-data	the filename for the transaction data set transmitted	including drive letter and directory name with filename if needed	in Request; M	used in file transmittal of any transaction data sets; and, used for posting back all transaction value pairs for a transmittal that had decryption-related errors.
input-format	descriptor of the data format used for the file transmitted	as defined by QEDM	in Request; M	NAESB standard format indicator used in file transmittal
receipt-disposition-to	the party to receive receipts, the value should be the same as the 'from'	Common Code Identifier format	in Request; M	used in file transmittal and in posting error notifications
receipt-report-type	type of receipt type being requested by Sender	gisb-acknowledgement-receipt	in Request; M	used in file transmittal and in posting error notifications
receipt-security-selection	used to request signed receipts	signed-receipt-protocol=required,pgp-signature;signed-receipt-micalg=required,md5	in Request; MA	used in file transmittal and in posting error notifications
refnum	used by the party to assign a message identifier unique over all time for tracing purposes. For the Sender, this ID should not be duplicated for resends.	Maximum 40 character integer value	in Request; MA	May be used by Sender to send tracking information to a recipient. Use of this data element is by mutually agreed. This data element is conceptually similar to a Message-ID filed within RFC 822.
refnum-orig	for original send, refnum-orig is identical to refnum. for resend, refnum-orig is the refnum of the original package.	Maximum 40 character integer value	In Request; MA	Used in conjunction with refnum.
request-status	status describing success or failure of transmission at recipient Server	ok; EEDM###:error description; WEDM###:warning description. see Table A, 'Internet EDM Standard Error Codes and Messages'	in Response; M	'ok' is returned if all is fine with processing; error messages/warnings and their related descriptions are returned if problems were encountered in processing.

Business Name	Definition	Format	Usage*	Condition
server-id	uniquely identifies the Server processing the transaction	domainname or hostname.domainname; no embedded spaces allowed	in Response; M	displayed in the HTTP Response and posted back for any decryption-related errors
time-c	the time file transfer is complete at the Server	yyyymmddhhmmss	in Response; M	displayed in the HTTP Response and posted back for any decryption-related errors; refer to QEDM for quadrant-specific use
time-c-qualifier	delta from UTC (ref ISO 8601)	-ZZ; +ZZ	in Response; MA	displayed in the HTTP Response and posted back for any decryption-related errors; refer to QEDM for quadrant-specific use
to **	the party the transaction was sent to	Common Code Identifier format	in Request; M	used in file transmittal and displayed in HTTP Response and posted back for any decryption-related errors
transaction-set	name of the document type being sent	8 character code; refer to NAESB REQ Implementation Guide, Related Standards Tab, Hypertext Transfer Protocol (HTTP) section, HTTP transaction-set Code Values table.	in Request; MA	used in file transmittal
trans-id	sequential number assigned to the transaction by the Server upon processing before being passed to the decryption process	integer up to 15 characters in length	in Response; M	displayed in the HTTP Response and posted back for any decryption-related errors
version	the NAESB Internet ET version being used by the Sender	numeric, decimal notation (e.g. 1.6)	in Request; M	used in file transmittal and in posting error notifications

*The **Usage** column defines whether the element appears in the HTTP Request (Client-generated) or the HTTP Response (Server-generated), the order in which the element appears in the data stream, and whether the field is Mandatory (M) or Mutually-Agreed-To (MA).

** Common Code Identifier

SENDING INTERNET ET PACKAGES

General Flow

The following is an example of the steps necessary to send an Internet ET package:

1. Open HTTP connection
2. Check connection status. If in error, re-queue package according to Internet ET standards. This check should be performed here and throughout the following processes.
3. Post, including a) Authentication, b) Send multipart form, c) Receive HTTP Response data
4. Check connection status. If in error re-queue package according to Internet ET standards
5. Check HTTP status code (200 is good, less than 300 may be acceptable). If status is not successful re-queue package according to Internet ET standards
6. Close connection - wait for other end to close in a reasonable time
7. Parse HTTP Response data elements
8. If request-status ok, then log success
9. If request-status error, then log error
10. If no valid request-status re-queue package according to Internet ET standards
11. Remove package from sending queue when successful or when failed completely

If trading partners agree to implement signed receipts, then the sending party must include the 'receipt-security-selection' data element in the posted data. The receiving party must digitally sign the 'gisb-acknowledgement-receipt' and encapsulate the 'gisb-acknowledgement-receipt' and digital signature body parts within a MIME envelope with a 'content-type' of 'application/pgp-signature'.

Use of Refnum and Refnum-orig

These data elements are mutually-agreed, so parties must agree to use these data elements.

The first time a package is sent the refnum and refnum-orig should be identical 40-digit or less integers. The refnum data element is always unique over time.

If a party does not receive the NAESB response, the package should be resent with a new refnum, and with the refnum-orig equal to the original refnum used in the initial transmittal of the package.

Refnum and Refnum-orig Example:

<u>Package Send</u>	<u>refnum</u>	<u>refnum-orig</u>
<u>First send</u>	<u>123467890123456</u>	<u>123467890123456</u>
<u>First resend</u>	<u>223467890123457</u>	<u>123467890123456</u>
<u>Second resend</u>	<u>323467890123458</u>	<u>123467890123456</u>

Using an Interactive Browser for Internet ET

Electronic packages can be uploaded to a trading partner using an interactive browser secured using SSL 128-bit encryption. Sending electronic packages via an interactive browser is ideal for a small volume of package transfers, or as a back-up method to any batch or automated process.

To use an interactive browser to upload data, an HTML document must be created with an HTML <FORM> element that allows the Sender to type in any necessary data elements, such as 'to', 'from', 'input-format', and the name of the file to be uploaded. When the user submits the form, an HTTP POST is sent to the Server with the package, which includes the uploaded file and the required data elements.

The following example is an HTML document with a form that specifies the POST method and contains the required data elements. This type of HTML form could be used with any browser that supports multipart POST with a file upload.

EXAMPLE: HTML DOCUMENT WITH A FORM FOR MULTIPART POST USING AN INTERACTIVE BROWSER:

```

<HTML><HEAD><TITLE>NAESB Internet ET Package Upload</TITLE><H1><CENTER>NAESB Internet ET
Package Upload</CENTER></H1></HEAD>
<BODY><HR>
<FORM ENCTYPE="multipart/form-data" ACTION="http://www.target.server/cgi-bin/upload.exe"
METHOD="POST">
Enter Common Code Identifier for 'From' and 'To':
From:
<INPUT TYPE="text" NAME="from" SIZE=20 VALUE=""><br>
To:
<INPUT TYPE="text" NAME="to" SIZE=20 VALUE=""><br>
NAESB Internet ET Version:
<INPUT TYPE="text" NAME="version" SIZE=5 VALUE="1.6"><br>
Deliver Receipt To:
<INPUT TYPE="text" NAME="report-disposition-to" SIZE=20 VALUE=""><br>
Receipt Type:
<INPUT TYPE="text" NAME="receipt-report-type" SIZE=30
VALUE="gisb-acknowledgement-receipt"><br>

IF requesting signed receipts also include: Receipt Type:
<INPUT TYPE="text" NAME="receipt-security-selection" SIZE=30
VALUE="signed-receipt-protocol=required, pgp-signature; signed-receipt-micalg=required,
md5"><br>
Format of this file:
<INPUT TYPE="text" NAME="input-format" SIZE=6 VALUE="X12"><br>
Send this file:
<INPUT NAME="input-data" TYPE="FILE"><br>
<INPUT TYPE="submit" VALUE="Send File"><br>
</FORM>
</BODY></HTML>

```

The important characteristics of the form within the HTML document are:

- ENCTYPE= specifies the encoding type. The 'multipart/form-data' encoding type is identified as the standard encoding methodology.
- ACTION= specifies the URL that will receive the uploaded data. The TEW or TPA identifies the URLs for both parties.
- METHOD= specifies the HTTP protocol method. 'POST' has been defined as the Internet ET standard method.
- <INPUT ...>. HTML INPUT elements include the required data elements such as 'from', 'to', and 'input-format'. Refer to the data dictionary for the complete list of required data elements.

When a user selects the 'Send File' button, the interactive browser will take the values entered in the input fields and reformat them into a data stream, formatted according to the encoding type. The file identified for upload is opened and its contents are included in the data stream. The data stream is then sent to the URL specified by '**ACTION=**', which indicates a Server Receiving script or program written to receive the package.

Using a Batch Browser for Internet ET

A batch browser is used by companies that want to automate their transport processes and/or prefer to minimize human involvement. A batch browser is initiated by a program or a script.

A batch browser can be created via custom programming. A batch browser is coded to perform the same formatting as an interactive browser, formatting a data stream that conforms to the HTTP and Internet ET protocols. A batch browser must be

coded as a 'TCP sockets' program. See the section 'Writing a Batch Browser'.

Authentication

Userids and passwords must be base64-encoded. HTTP basic authentication includes a 'userid' and 'password'. Interactive browsers include a basic authentication feature that automatically prompts for 'userid' and 'password'. In a batch browser, the authentication must be specifically coded. The 'userid' and 'password' are to be base64-encoded within the document header. Base64-encoding utilities are readily available on the Internet as either public domain software or commercial libraries.

Server Response

The Server will send a 'gisb-acknowledgement-receipt' in the HTTP Response to the Client before dropping the Client's connection. If the transacting parties agree to use signed receipts, the Server applies a digital signature to the 'gisb-acknowledgement-receipt' and encapsulates the entire package in a MIME envelope of 'content-type: application/pgp-signature'.

The 'gisb-acknowledgement-receipt' returned from the Server contains the 'time-c' and the 'time-c-qualifier' (where applicable) Receipt timestamps that are recorded when the final byte from the package upload is received and stored. This Receipt timestamp is the official timestamp regarding transaction turnaround deadlines as defined in Internet ET and QEDM standards. This timestamp and all other pertinent package transmittal information should be logged by the Receiver when the posted package is stored on the Server, and logged by the Client. Errors or warnings should be logged at both the Client and Server.

Sender HTTP Request Data Elements

The HTTP Request will provide all required data elements in the ORDER DEFINED BELOW. Any 'mutually-agreed-upon' data elements will follow the required data elements in the data stream. Refer to the section 'Data Dictionary for Internet ET' for descriptions of these data elements.

Required Data Elements, Listed in the Required Order:

1. from
2. to
3. version
4. receipt-disposition-to
5. receipt-report-type
6. input-format
7. input-data

Mutually Agreed Upon Data Elements

8. transaction-set
9. receipt-security-selection
- 10.refnum
- 11.refnum-orig

Writing a Batch Browser

A batch browser Client needs to simulate the actions of an interactive browser Client. As stated earlier, the interactive browser Client will take the HTML form, reformat the information according to the HTTP protocol, then send the data stream to the Server. The reformatting adds a header and places field delimiters around the data items.

A batch browser needs to produce the same kind of data stream and, therefore, writing a batch browser requires some specific knowledge of the HTTP protocol.

EXAMPLE: A TYPICAL HEADER SENT TO THE SERVER

```
POST /cgi-bin/AS2dispatcher HTTP/1.1
Referer: http://www.get.a.life/upl.htm
Connection: Keep-Alive
User-Agent: brow v0.1 XYZ Corp.
Host: localhost
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
content-type: multipart/form-data; boundary=-----87453838942833
Content-Length: 5379
```

POST Line - In the example above, the first line indicates the POST method was used and identifies which Receiving Program to call:

```
POST /cgi-bin/AS2dispatcher HTTP/1.1
```

Content Type - The 'content-type' line indicates that the encoding method is multipart, and identifies the character string used as the boundary.

```
content-type: multipart/form-data; boundary=-----87453838942833
```

Boundary String - The 'boundary=' identifies the string that will appear between each field as a delimiter. In this example, the boundary is comprised of 27 hyphen characters followed by a number.

```
content-type: multipart/form-data; boundary=-----87453838942833
```

The boundary can be ANY character string that you choose. The string used CANNOT OCCUR ANYWHERE ELSE IN THE PACKAGE BEING SENT. This is usually accomplished by using either the system clock or a random number so that even if by some remote chance the string appears in the document it would not appear in any re-transmission of the file. It is strongly recommended that a relatively long string be used as a boundary.

The boundary string, when used as a separator, REQUIRES TWO HYPHEN CHARACTERS APPENDED TO THE FRONT of the string. The LAST boundary required in the form is TWO HYPHEN CHARACTERS APPENDED TO THE BACK of the separator boundary, used to indicate to the Server program that this is the end of the data.

```
-----87453838942833--
```

Content Length - The 'content-length' value should match the number of bytes contained in the entity body including the characters in the boundary lines, variable content, blank lines, etc. 'content-length' indicates to the Server how much data are going to come after this point. In the example above, the content length is:

```
Content-Length: 5379
```

Envelope / Required Data Elements. The envelope information for the package ('to', 'from', etc) is included in a series of boundaries that include the 'content-disposition' and 'name=' qualifiers, followed by the data element value. The example below includes the 'from' field as '123456789' and the 'to' field as '234567890'.

```
-----87453838942833
content-disposition: form-data; name="from"

123456789
-----87453838942833
content-disposition: form-data; name="to"

234567890
```

The 'content-disposition' identifier defines that 'form-data' is contained in the element. The 'name=' identifier defines the name of the data element. These data element names must match the name specified by Internet ET Data Dictionary. The 'name=' identifier is not completely relevant since the fields should be present in the correct order, but this field should be checked to verify the validity of the form content.

The actual data value of the field is always preceded by a blank line. This is typically used as a marker for the Server program to indicate that a data value will follow. For example, note the blank line preceding 'X12' in the example. In most programming libraries and commercial products the starting delimiter is '\r\n\r\n' (C notation).

```
-----87453838942833
content-disposition: form-data; name="version"

1.64
-----87453838942833
content-disposition: form-data; name="receipt-disposition-to"

123456789)
-----87453838942833
content-disposition: form-data; name="receipt-report-type"

gisb-acknowledgement-receipt
-----87453838942833
content-disposition: form-data; name="input-format"

x12
```

Payload. The content or 'payload' (EDI, etc) is encrypted and included in its own boundary section.

The data field containing the Internet ET payload file has two extra identifiers. The 'filename=' element indicates the name of the file sent from by the Sender. In the example the name of the file is 'c:\temp\smallnom.bin'.

```
content-disposition: form-data; name="input-data"; filename="c:\temp\smallnom.bin"
```

The 'content-type' element indicates the type of the data being transmitted according to accepted Internet standards.

```
content-type: multipart/encrypted; boundary=--boundary2--200309090001;
protocol="application/pgp-encrypted"
```

Note that encrypted files can be multipart also, which means they will have their own boundary string.

```
-----87453838942833
content-disposition: form-data; name="input-data"; filename="c:\temp\smallnom.bin"
content-type: multipart/encrypted; boundary=--boundary2--200309090001;
protocol="application/pgp-encrypted"

----boundary2--200309090001
content-type: application/pgp-encrypted

Version: 1

----boundary2--200309090001
content-type: application/octet-stream

-----BEGIN PGP MESSAGE-----
Version: PGP 6.5

hQCMaZRG1pEOIOvdAQP+JMr0m/9+8yOL60Z9Vr6fFV81FCExB/o0xmwiMkiwYsHsz0e8sb7ErC340MrNA/dw3taGMjmI+C
XYRF/PLEdg1NZE1ZCtNeL4YdIHAMLWwODG1QxhSucz8rMSgQ5mZzc0JwBdWLW70efgsu/9U1juJjYcluZ6C03eFQv/43fk
B+a1ATtgydxX4g8QK664ad+Jo/XUICSmWBL66fqJR1KLeLf4wTaqGy174Aq48WpwwglEh785zC03UAW0qg0ugMt86dPeyd
91e2JigqwDYef/DYEKD0J9BGiGpS/uAupNKj80cp2IwClxKOGUbxpVNOntqWHS/GntegvDE//ewCxDxsnmQS95p01141
QZ1RqbeNaqx2Dq/ra9g65HNchOCzju15Vi8HHf6Yhg2WnROe+npByyCue6rihgqNVOJwj0Cvzpb4JE+gMDf3q4ISUblFv7/
+/SSFHddndhC5YTpqf1Bc3B07hiLmtTXqNit31EbX9UVE1ObzSa9ZhxbC6/eS17Nuf5ZTDsh9nrk+QQJ6FeC9W4cqXLj7I
ZySaR08Vtff+4ktqeuHYust4kSpnk027aw40/5jomUkfb22CAe4=
=Oiuo
-----END PGP MESSAGE-----
----boundary2--200309090001--
```

Boundary String Terminators - Each multipart stream must be terminated with the boundary string terminator. After the contents of the last data field, the boundary string and the required two-hyphen terminator indicate the end of the multipart encrypted payload. A second boundary terminator string indicates the end of the package:

```
----boundary2--200309090001--
-----87453838942833--
```

EXAMPLE: AN X12 EDI FILE ENCRYPTED WITH PGP

```
content-type: multipart/encrypted; boundary=--boundary2--200309090001;
protocol="application/pgp-encrypted"

----boundary2--200309090001
content-type: application/pgp-encrypted

Version: 1

----boundary2--200309090001
content-type: application/octet-stream

-----BEGIN PGP MESSAGE-----
Version: PGP 6.5

hQCMaZRG1pEOIOvdAQP+JMr0m/9+8yOL60Z9Vr6fFV81FCExB/o0xmwiMkiwYsHsz0e8sb7ErC340MrNA/dw3taGMjmI+CX
YRF/PLEdg1NZE1ZCtNeL4YdIHAMLWwODG1QxhSucz8rMSgQ5mZzc0JwBdWLW70efgsu/9U1juJjYcluZ6C03eFQv/43fkB
+a1ATtgydxX4g8QK664ad+Jo/XUICSmWBL66fqJR1KLeLf4wTaqGy174Aq48WpwwglEh785zC03UAW0qg0ugMt86dPeyd9
1e2JigqwDYef/DYEKD0J9BGiGpS/uAupNKj80cp2IwClxKOGUbxpVNOntqWHS/GntegvDE//ewCxDxsnmQS95p01141Q
Z1RqbeNaqx2Dq/ra9g65HNchOCzju15Vi8HHf6Yhg2WnROe+npByyCue6rihgqNVOJwj0Cvzpb4JE+gMDf3q4ISUblFv7/
+/SSFHddndhC5YTpqf1Bc3B07hiLmtTXqNit31EbX9.UVE1ObzSa9ZhxbC6/eS17Nuf5ZTDsh9nrk+QQJ6FeC9W4cqXLj7I
ZySaR08Vtff+4ktqeuHYust4kSpnk027aw40/5jomUkfb22CAe4=
=Oiuo
-----END PGP MESSAGE-----
----boundary2--200309090001--
```

EXAMPLE: AN X12 EDI DATA STREAM BEFORE ENCRYPTION:

```
content-type: application/EDI-X12

ISA~00~ ~01~AAA6300300~14~1234567890000 ~14~2345678900000
... more data from the X12 file...
IEA~1~000003616
```

EXAMPLE: A COMPLETE ELECTRONIC PACKAGE DATA STREAM

```
POST /cgi-bin/AS2dispatcher HTTP/1.1
Referer: http://www.get.a.life/upl.htm
Connection: Keep-Alive
User-Agent: brow v0.1 XYZ Corp.
Host: localhost
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
content-type: multipart/form-data; boundary=-----87453838942833
Content-Length: 5379

-----87453838942833
content-disposition: form-data; name="from"

123456789
-----87453838942833
content-disposition: form-data; name="to"

234567890
-----87453838942833
content-disposition: form-data; name="version"

1.46
-----87453838942833
content-disposition: form-data; name="receipt-disposition-to"

123456789
-----87453838942833
content-disposition: form-data; name="receipt-report-type"

gisb-acknowledgement-receipt
-----87453838942833
content-disposition: form-data; name="input-format"

X12
-----87453838942833
content-disposition: form-data; name="input-data"; filename="c:\temp\smallnom.bin"
content-type: multipart/encrypted; boundary=--boundary2--200309090001;
protocol="application/pgp-encrypted"

----boundary2--200309090001
content-type: application/pgp-encrypted

Version: 1

----boundary2--200309090001
content-type: application/octet-stream

-----BEGIN PGP MESSAGE-----
Version: PGP 6.5

hQCMaZRG1pEOIOvdAQP+JMr0m/9+8yOL60Z9Vr6fFV81FCExB/o0xmwiMkiwYsHsz0e8sb7ErC340MrNA/dw3taGMjmI+C
XYRF/PLEdg1NZE1ZCtNeL4YdIHAMLWwODG1QxhSucz8rMSgQ5mZzc0JwBdWLW70efgsu/9U1juJjYcluZ6C03eFQv/43fk
B+alAtTgydxX4g8QK664ad+Jo/XUICSmWBL66fqJR1KLeLf4wTaqGy174Aq48Wpwwg1Eh785zC03UAw0qg0ugMt86dPeyd
91e2JigqwDYef/DYEKD0J9BGiGpS/uAupNKj80cp2IWClxKOGUbxpVNOntqWHS/GntegvDE/7/ewCxXsnmQS95pO1141
QZ1RqbeNaqx2Dq/ra9g65HNchOCzjul5Vi8HHf6Yhg2WnRo+npByyCue6rihgqNVOJwj0cVzpb4JE+gMdf3q4ISUblFv7
/+SSFHDDnhdC5YTpqf1Bc3B07hiLmtTXqNit31EbX9UVElObzSa9Zhx6C6/eS17Nuf5ZTDsh9nrk+QQJ6FeC9W4cqXLj7I
ZySaR08Vtff+4ktqeuHust4kSpnk027aw40/5jomUkfb22CAe4=
=Oiuo
-----END PGP MESSAGE-----
----boundary2--200309090001--
-----87453838942833--
```

RECEIVING INTERNET ET PACKAGES

General Flow

The following is an example of the steps necessary to receive an Internet ET package:

1. Parse multi-part form
2. Validate HTTP Request data elements
3. If HTTP Request data elements in error, return appropriate Internet ET standard error code in the HTTP Response data elements
4. Save data
5. Create 'gisb-acknowledgement-receipt'
6. If using signed receipts, produce a digital signature over the 'gisb-acknowledgement-receipt' created in step 5.
7. Encapsulate the 'gisb-acknowledgement-receipt' and digital signature body parts in a 'Content-Type' of 'multipart/signed envelope'
8. Return HTTP Response with the 'gisb-acknowledgement-receipt' object back to Client
9. Close connection
10. Log final results
11. Route data file to the next process based upon 'input-format'

Overview of Web Server Receiving Programs

The HTTP Server receives the POST and calls the appropriate Receiving script or program to:

- parse the incoming HTTP Request
- create the Receipt timestamp using the current date and time
- create an HTML Response to the Client

An Internet ET Receiving Program may be implemented using a variety of technologies and techniques, including Active Server Pages (ASP), Common Gateway Interface (CGI), Java Server Pages (JSP), Java Servlets, and Personal Home Pages (PHP). The Internet ET is supported by most commercially available Web/HTTP servers.

The Receiving Program and Process

The Receiving Program must be able to parse the multi-part form. It accomplishes this by finding the boundary string in the 'content-type' header and scanning for its occurrences further within the uploaded stream. Upon finding these boundary strings, the program must next determine the 'content-disposition' for each data element. This allows detection of the required text elements as well as the Internet ET payload file.

The Receiving Program only stores the payload file and is not concerned with the content of the payload file, which is encrypted. It will use the 'content-length' to determine how much data to expect in the body of the package.

A Receiving process requires an executable program or module that is called by the Server when it is identified by a POST operation.

When the Server receives a POST it will first read the header and populate environment variables before calling the Receiving Program. Most HTTP servers read header variables and populate environment variables. Check your HTTP server documentation for more information.

EXAMPLE: A SAMPLE HTTP POST HEADER

```
POST /cgi-bin/AS2dispatcher HTTP/1.1
Referer: http://www.get.a.life/upl.htm
Connection: Keep-Alive
User-Agent: brow v0.1 XYZ Corp.
Host: localhost
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
content-type: multipart/form-data; boundary=-----87453838942833
Content-Length: 5379
```

After reading the HTTP header information, the Server will buffer the remaining data transmitted and call the Receiving Program specified in the POST statement. Do not assume that the Receiving Program is called as soon as the header is read, which can impact your receipt timestamp. The more common implementations buffer the entire transmission before calling the program. Check your server implementation if this characteristic is important to you.

The Receiving Program will have the following data stream available, and will have most of the header data available in environment variables.

EXAMPLE: DATA STREAM AVAILABLE TO RECEIVING PROGRAM

```

-----87453838942833
content-disposition: form-data; name="from"
123456789
-----87453838942833
content-disposition: form-data; name="to"
234567890
-----87453838942833
content-disposition: form-data; name="version"
1.64
-----87453838942833
content-disposition: form-data; name="receipt-disposition-to"
123456789
-----87453838942833
content-disposition: form-data; name="receipt-report-type"
gisb-acknowledgement-receipt
-----87453838942833
content-disposition: form-data; name="input-format"
X12
-----87453838942833
content-disposition: form-data; name="input-data"; filename="c:\temp\smallnom.bin"
content-type: multipart/encrypted; boundary=--boundary2--200309090001;
protocol="application/pgp-encrypted"
----boundary2--200309090001
content-type: application/pgp-encrypted
Version: 1
----boundary2--200309090001
content-type: application/octet-stream
-----BEGIN PGP MESSAGE-----
Version: PGP 6.5
hQCMazRGlpeOIovdAQP+JMr0m/9+8yOL60Z9Vr6fFV81FCExB/o0xmwimkiwYsHsz0e8sb7ErC340MrNA/dw3taGMjmI+C
XYRF/PLEdg1NZE1ZCtNeL4YdIHAMLWwODG1QxhSucz8rMSgQ5mZzcOJwBdWLW70efgsu/9U1juJjYcluZ6C03eFQv/43fk
B+alAtTgydxX4g8QK664ad+Jo/XUICSmWBL66fqJR1KLeLf4wTaqGy174Aq48Wpwwg1Eh785zC03UAW0qg0ugMt86dPeyd
91e2JigqwDYef/DYEKD0J9BGiGpS/uAupNKj8Ocp2IWClxKOGUbxpVNOntqWHS/GntegvDE/7/ewCxDxsnmQS95p01141
QZ1RQbeN.aqx2Dq/ra9g65HNchOCzjul5Vi8HHf6Yhg2WnROe+npByyCue6rihqgNVOJwj0cVzpb4JE+gMDf3q4ISUb1Fv
7/+SSFHDDhdhC5YTpqf1Bc3B07hiLmtTXqNit31EbX9UVE1ObzSa9ZhxbC6/eS17Nuf5ZTDsh9nrk+QQJ6FeC9W4cqXLj7
IZySaR08Vtff+4ktqeuHysT4kSpnk027aw40/5jomUkfb22CAe4=
=Oiuo
-----END PGP MESSAGE-----
----boundary2--200309090001--
-----87453838942833--

```

This Receiving Program should check for basic validity in the environment variables and the data stream, and then parse the variables/data from the format. Data validations should include:

- The 'REQUEST_METHOD' environment variable is 'POST'.
- The 'CONTENT_TYPE' environment variable should be 'multipart/form-data' and the boundary, which cannot appear anywhere in the transaction being sent.
- The input stream should support binary mode to accommodate encrypted files.
- Each data element should be preceded by the boundary with the required two hyphen characters appearing before it.
- Each data element should contain the correct name on the 'content-disposition' line.
- Each data element should have a blank line ('\r\n\r\n' in C+ notation) before the start of the data.
- All tag values in the HTTP header should be evaluated in a case insensitive manner.
- Improperly formatted input. Finding the end of the stream using both 'content-length' and the boundary string terminator end mark is a good method to

detect improperly formatted input.

Acknowledgement Receipt: 'gisb-acknowledgement-receipt'

The Acknowledgement Receipt ('Receipt') is critical to non-repudiation and business process timing. Immediately after the Receiving Program receives the last byte of data from the Sender, the Receiving Program should record the time and construct a 'gisb-acknowledgement-receipt'. This Receipt is sent from the Receiving Program to the Client prior to closing the HTTP connection.

The Receipt is a MIME-formatted text stream that includes the HTTP Response data elements (time-c, time-c-qualifier for REQ/RGQ, request-status, server-id, trans-id) in a 'multipart/report' MIME envelope.

If signed Receipts are used, the 'gisb-acknowledgement-receipt' including the 'multipart/report' envelope, is digitally signed, producing an 'application/pgp-encrypted' body part. Both the 'multipart/report' 'gisb-acknowledgement-receipt' and the 'application/pgp-signature' body parts are placed in a 'multipart/signed' envelope and the entire package is returned to the Sender.

The Receipt name 'gisb-acknowledgement-receipt' retains the 'gisb-' prefix to assure compatibility with legacy GISB EDM implementations. The name is only used in the 'report-type' data element for the MIME part.

Additional Receiving Program Functions

- All data element names of the HTTP Request and Response fields will be in lower case. Note that the Internet ET standard format file contained in the Request and Response may follow a different standard.
- Carriage returns and line feeds will be ignored in all files.
- A field delimiter of '*' will be used in the HTTP Response. Please refrain from displaying a '*' anywhere else in the response so as not to confuse programs that need to parse on this basis.
- No spaces should surround the equal sign or the field delimiter.
- The required data elements must appear first in the HTTP Response and in the order specified. Additional information can be included after the required elements at the server's discretion.
- The first occurrence of the field name within the response will contain the value.
- If an HTML response is given, all data must be presented in a user-readable fashion. For example, if the required machine-readable fields are embedded in comments, another representation of these fields must be presented to the user.

Receiving Process URL Implementation Guidelines

Each company must offer at least one URL to accept files using Internet ET. Companies can offer multiple URLs. Though companies are free to construct a Web site with multiple 'single-purpose' URLs (e.g. nominations.xyzcorp.com; enrollments.xyzcorp.com) NAESB recommends the use of one 'general-purpose' URL.

The Receiving Program may initiate error notifications after the 'gisb-acknowledgement-receipt' is sent (e.g. file decryption errors). Error notifications posted to the Sender would be directed to the Sender's general-purpose URL.

All URLs that will be required for use in the Internet ET process must be agreed to and defined in a Technical Exchange Worksheet (TEW) or a Trading Partner Agreement (TPA).

HTTP Response 'gisb-acknowledgement-receipt' Data Elements

Required HTTP Response Data Elements (listed in the required order)	
WGQ	REQ/RGQ
time-c	time-c
request-status	time-c-qualifier
server-id	request-status
trans-id	server-id
	trans-id

Examples of HTTP Response Required Data Elements:

EXAMPLE: RESPONSE, SUCCESSFUL, MULTIPART FORMAT:

```

content-type: multipart/report; report-type="gisb-acknowledgement-receipt";
boundary="NAESB7867"

--NAESB7867
content-type: text/html

<HTML><HEAD><TITLE>Acknowledgement Receipt Success</TITLE></HEAD> <BODY><P>
time-c=19960619082855*
request-status=ok*
server-id=coolhost*
trans-id=234423897*
</P> </BODY></HTML>
--NAESB7867
content-type: text/plain

time-c=19960619082855*
request-status=ok*
server-id=coolhost*
trans-id=234423897*
--NAESB7867--
    
```

EXAMPLE: RESPONSE, SUCCESSFUL, MULTIPART FORMAT, TIME-C-QUALIFER FOR TIME ZONE:

```
content-type: multipart/report; report-type="gisb-acknowledgement-receipt";
boundary="NAESB7867"

--NAESB7867
content-type: text/html

<HTML><HEAD><TITLE>Acknowledgement Receipt Success</TITLE></HEAD> <BODY><P>
time-c=19960619082855*
time-c-qualifier=-05*
request-status=ok*
server-id=coolhost*
trans-id=234423897*
time-c-qualifer=-0400
</P> </BODY></HTML>
--NAESB7867
content-type: text/plain

time-c=19960619082855*
time-c-qualifier=-05*
request-status=ok*
server-id=coolhost*
trans-id=234423897*
time-c-qualifer=-0400
--NAESB7867--
```

EXAMPLE: RESPONSE, ERROR, MULTIPART FORMAT:

```
content-type: multipart/report; report-type="gisb-acknowledgement-receipt";
boundary="NAESB7866"

--NAESB7866
content-type: text/html

<HTML><HEAD><TITLE>Acknowledgement Receipt Error</TITLE></HEAD> <BODY><P>
time-c=19960619082855*
request-status=EEDM106: Invalid To Common Code Identifier*
server-id=coolhost*
trans-id=234423897*
</P> </BODY></HTML>
--NAESB7866
content-type: text/plain

time-c=19960619082855*
request-status=EEDM106: Invalid To Common Code Identifier*
server-id=coolhost*
trans-id=234423897*
--NAESB7866--
```

EXAMPLE: RESPONSE, WARNING, MULTIPART FORMAT:

```

content-type: multipart/report; report-type="gisb-acknowledgement-receipt";
boundary="NAESB7866"

--NAESB7866
content-type: text/html

<HTML><HEAD><TITLE>Acknowledgement Receipt Warning</TITLE></HEAD> <BODY><P>
time-c=19960619082855*
request-status=WEDM100: Transaction Set Sent, Not Mutually Agreed*
server-id=coolhost*
trans-id=234423897*
</P> </BODY></HTML>
--NAESB7866
content-type: text/plain

time-c=19960619082855*
request-status= WEDM100: Transaction Set Sent, Not Mutually Agreed *
server-id=coolhost*
trans-id=234423897*
--NAESB7866--
    
```

EXAMPLE: RESPONSE, SUCCESSFUL , SIGNED RECEIPT:

```

content-type:multipart/signed; micalg=pgp-md5; protocol="application/pgp-signature";
boundary=--boundary2--200309090001

----boundary2--200309090001

content-type: multipart/report; report-type="gisb-acknowledgement-receipt";
boundary="NAESB7867"

--NAESB7867
content-type: text/html

<HTML><HEAD><TITLE>Acknowledgement Receipt Success</TITLE></HEAD> <BODY><P>

time-c=19960619082855*
request-status=ok*
server-id=coolhost*
trans-id=234423897*

</P> </BODY></HTML>

--NAESB7867
content-type: text/plain.
time-c=19960619082855*
request-status=ok*
server-id=coolhost*
trans-id=234423897*
--NAESB7867--
----boundary2--200309090001
content-type: application/pgp-signature

-----BEGIN PGP MESSAGE-----

Version: 2.6.26.5

iQCVAwUBMJrRF2N9oWBghPDJAQE9UQQAt17LuRVndBjrk4EqYBib3h5QXIX/LC//JV5bNvkZIGPICEmI5iFd9boEgvpirH
tIREEqLQRkYNoBActFBZmh9GC3C041WGquMbrbxc+nIs1TIK1A08rVi9ig/2Yh7LFrK5Ein57U/W72vgSxLhe/zhdfo1T9
BrnHOxEa44b+EI=
=ndaj

-----END PGP MESSAGE-----

----boundary2--200309090001--
    
```

EXAMPLE: HTML FORMAT RESPONSE, SUCCESSFUL:

```

<html><head><title>Upload OK</title></head>
<body>
<!-- time-c=19960123203618*-->
<!-- request-status=ok* -->
<!-- server-id=coolhost*-->
<!-- trans-id=232323897*-->
<h1>Upload OK</h1>
<b>File Saved at (time-c):</b> 19960123203618<br>
<b>Status (request-status):</b>ok<br>
<b>Server (server-id):</b>coolhost<br>
<b>Transaction ID (trans-id):</b>232323897<br>
</body></html>

```

SENDING INTERNET ET ERROR NOTIFICATIONS

When a Client sends an Internet ET package to a Server, the Server responds with a Receipt. Further back-office processing (e.g. decryption) may be required, and additional errors may be found.

Error Notification transactions are used to communicate transport errors found by the Receiver after the initial receipt is sent to the Sender.

Errors from translation and other back-office processing are outside the scope of the Internet ET.

When a file passes the decryption step, no error notification is sent back to the Client. If the decryption step fails, an error notification must be sent to the Client.

The Error Notification format applies to the posting of an error message after the Sender's session has been disconnected. This error notification is used only if the original HTTP Response is returned with an 'ok'.

Additionally, trading partners are permitted to use digitally-signed error notifications, if both parties mutually agree to do so.

Required Error Notification Data Elements

The data elements for the error notification are the same as those described in the Section 'Sending Transactions', with the exception of the 'input-format' and 'input-data' elements. The file containing the data elements for error notification should not be encrypted.

Required Data Elements for Error Notification (listed in the required order):

1. 'from'
2. 'to'
3. 'input-format'

Error Notification 'input-data' Element Specifications:

- The file containing the data elements for error notification should not be encrypted.
- All data element names will be in lower case in the Error Notification.
- Carriage returns and line feeds will be ignored in all files.
- A field delimiter of '*' will be used in the Error Notification. Please refrain from

displaying a '*' anywhere else in the error notification so as not to confuse programs that need to parse on this basis.

- No spaces should surround the equal sign or the field delimiter.
- The required data elements must appear first in the response.
- Additional information can be included after the required elements at the server's discretion.
- The first occurrence of the field name within the response will contain the value.
- An error notification contains two body parts nested within a multipart/report outer envelope with the content-type of 'gisb-error-notification'.
- The first body part contains human readable content in HTML. The second body part contains machine readable content in plain text. Additionally, consenting trading partners can mutually agree to digitally sign error notifications.
- If digital signatures are used, the multipart/report containing the Error Notification is used to create a digital signature body part, identified by a 'content-type' of application/pgp-signature. Both the multipart/report Error Notification and application/pgp-encrypted digital signature body parts are combined in a multipart/signed envelope.

EXAMPLE: ERROR NOTIFICATION INTERNET ET PACKAGE:

```

POST /cgi-bin/AS2dispatcher HTTP/1.1
Referer: http://www.acmeenergy/upl.htm
Connection: Keep-Alive
User-Agent: brow v0.1 XYZ Corp.
Host: localhost
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
content-type: multipart/form-data; boundary=-----87453838942833
Content-Length: 1958
-----87453838942833
content-disposition: form-data; name="from"

234567890
-----87453838942833
content-disposition: form-data; name="to"

123456789
-----87453838942833
content-disposition: form-data; name="version"

1.6
-----87453838942833
content-disposition: form-data; name="receipt-disposition-to"

123456789
-----87453838942833
content-disposition: form-data; name="receipt-report-type"

gisb-acknowledgement-receipt
-----87453838942833
content-disposition: form-data; name="input-format"

error
-----87453838942833
content-disposition: form-data; name="input-data"; filename="c:\temp\error.not"
content-type: multipart/report; report-type="gisb-error-notification"; boundary="NAESB7868"

--NAESB7868
content-type: text/html

<HTML><HEAD><TITLE>Error Notification</TITLE></HEAD> <BODY><P>
orig-from=123456789*
orig-to=234567890*
orig-input-format=X12*
resp-time-c=19960619102855*
resp-server-id=coolhost*
resp-trans-id=234423897*
request-status=EEDM601: Public Key Invalid*
comments=Please contact 1-800-555-1212 for correct public key*
</P> </BODY></HTML>

--NAESB7868
content-type: text/plain

orig-from=123456789*
orig-to=234567890*
orig-input-format=X12*
resp-time-c=19960619102855*
resp-server-id=coolhost*
resp-trans-id=234423897*
request-status=EEDM601: Public Key Invalid*
comments=Please contact 1-800-555-1212 for correct public key*
--NAESB7868--
-----87453838942833--

Signed Error Notification

content-type:multipart/signed; micalg=pgp-md5; protocol="application/pgp-signature";
boundary=--boundary2--200309090001

----boundary2--200309090001

content-type: multipart/report; report-type="gisb-error-notification"; boundary="NAESB7868"

--NAESB7868
    
```

```

content-type: text/html

<HTML><HEAD><TITLE>Error Notification</TITLE></HEAD> <BODY><P>
orig-from=123456789*
orig-to=234567890*
orig-input-format=X12*
resp-time-c=19960619102855*
resp-server-id=coolhost*
resp-trans-id=234423897*
request-status=EEDM601: Public Key Invalid*
comments=Please contact 1-800-555-1212 for correct public key*

</P> </BODY></HTML>

--NAESB7868
content-type: text/plain

orig-from=123456789*
orig-to=234567890*
orig-input-format=X12*
resp-time-c=19960619102855*
resp-server-id=coolhost*
resp-trans-id=234423897*
request-status=EEDM601: Public Key Invalid*
comments=Please contact 1-800-555-1212 for correct public key*

--NAESB7868--
----boundary2--200309090001

content-type: application/pgp-signature
-----BEGIN PGP MESSAGE-----

Version: 6.5

iQCVAwUBMjrRF2N9oWBghPDJAJQE9UQQAtl7LuRVndBjrk4EqYBIb3h5QXIX/LC//JV5bNvkZIGPIcEmI5iFd9boEgvpirH
tIREEqLQRkYNoBActFBZmh9GC3C041WGquMbrbxc+nIs1TIKlA08rVi9ig/2Yh7LFrK5Ein57U/W72vgSxLhe/zhdfo1T9
BrnHOxEa44b+EI=
=ndaj

-----END PGP MESSAGE-----

----boundary2--200309090001--

```

Pre-validation before Decryption

Proper trapping of the range of decryption process errors listed in Table A (Internet EDM Standard Error Messages and Codes) may require program code which is external to the decryption algorithm. Some versions of the PGP software do not explicitly discriminate between EEDM601, EEDM602, EEDM603, and EEDM699 type errors.

Under such a circumstance, files inbound to the decryption process should be preprocessed to trap the errors not identified by the PGP version being used. For example, searching the file for the text strings 'BEGIN PGP MESSAGE' and 'END PGP MESSAGE' can quickly identify 'EEDM602 File not encrypted' and 'EEDM603 Encrypted file truncated' type errors when the implemented PGP version only identifies decryption success, invalid Public Key (EEDM601), and decryption failure (EEDM699).

SECURITY

Internet ET security requirements include four primary security aspects: data Privacy, data Integrity, Authentication, and Non-repudiation (PAIN).

- Data privacy: unauthorized parties cannot decipher the content of the data.
- Authentication: the Receiver is certain of the identity of the Sender.

- Data integrity: unauthorized parties cannot modify or corrupt the data.
- Non-repudiation: the Sender cannot deny ownership of the transaction if it was sent with their digital signature.

In general, these needs are met by using the Basic Authentication capability of the Web server and the encryption and digital signature capability of the Open PGP and PGP security application for securing transactions.

Understanding OpenPGP and PGP

Pretty Good Privacy (PGP) is the name of the chosen security application. OpenPGP is the Internet Engineering Task Force (IETF) standard version of PGP that excludes all patented algorithms, allowing free commercial use of the standard. Both OpenPGP and PGP use a Public Key/Private Key pair to secure and sign files for transfer. The Private Key must be known only to the company that generated it. The Public Key counterpart is shared with trading partners.

Each company must generate its Public Key and Private Key pair. The RSA key generation algorithm should be chosen for versions of PGP that offer alternatives. Implementers of OpenPGP should choose DSA and El Gamal when creating their key pair. The Public Keys should be distributed electronically to the company's trading partners. Private keys are not typically exchanged with trading partners. In the event that a Private Key needs to be exchanged, the exchange should occur in a secure manner such as postal or courier mail.

You must use the utmost care in protecting your Private Key. If an untrusted party has your Private Key, your security is compromised. It is recommended that a key size of 1024 be chosen when generating the key pair. This provides a significantly secure transaction.

When a company wishes to send transactions to its trading partner, it will use the partner's Public Key to encrypt the file. Encryption provides data privacy. Only the Private Key counterpart can decrypt this file.

When the sending party encrypts the file, it also uses its own Private Key to 'sign' the transaction. The receiving party can use the Sender's Public Key to verify the signature. The digital signature provides non-repudiation.

Encryption / Digital Signature

Encryption and digital signatures are applied to payload files before they are sent by the batch browser. The use of internal file or payload encryption such as X12.58 encryption is outside the scope of NAESB encryption standards but does not conflict with OpenPGP/PGP.

Encryption and digital signatures are created using OpenPGP, or on a mutually agreed basis, PGP version 2.6 or greater. Regardless of encrypting in a manual or automated fashion, it is essential that the correct Public Key of the trading partner be used to encrypt and just as essential that the correct Sender's own Private Key be used to digitally sign the file.

Digital signatures may also be applied, on a mutually-agreed-upon basis, to the HTTP Response by the Receiver of the package.

Decryption / Digital Signature Verification

After a package is received and processed by the Receiving Program, it is ready to be decrypted and have its digital signature verified. Given the correct userID for a trading partner, OpenPGP/PGP uses the appropriate key pair to encrypt, sign and decrypt. Upon request for signature verification, the OpenPGP/PGP will return a human-readable descriptive text such as DUNS number or company name.

When digital signatures are applied, on a mutually-agreed-upon basis, the HTTP Response received by the Sender of the transaction may be verified to ensure non-repudiation of receipt of the transaction.

Throughput Considerations

Encryption, digital signing, decryption and signature verification are all very CPU intensive. Companies anticipating large volumes of Internet ET traffic should research state-of-the-art techniques for scalability, including but not limited to:

- separating decryption and signature verification processing from web server receiving and processing
- passing secured or to-be-secured packages to a separate computer for security processing
- optimizing CPU and memory on security processing computers
- real-time or near real-time monitoring of website performance

Implementers of Internet ET sites should review and evaluate Domain Name Server (DNS) cache refresh intervals so as to ensure trading partner address changes are recognized on a timely basis.

Decryption and digital signature verification may not necessarily be processed by the Receiving Program prior to the 'gisb-acknowledgement-receipt' being sent to the Sender. As a result, the Sender may get an HTTP Response indicating a successful transfer but still not know if the file was successfully decrypted by the Receiver. Guidelines for communicating decryption errors found after the initial HTTP Response is sent are in Section 'Sending Error Notification Transactions' and Table A, 'Internet EDM Standard Error Codes and Messages'.

Security Requirements

Basic Authentication. Basic authentication, also known as realm one security, has been defined as one of the security standards for transmission on the Internet. The userID and password will be assigned by the server party according to site standards. The TPA must identify the userID and password for this security as well as procedures for changing the password, if applicable.

OpenPGP or PGP File Encryption. Payload files are encrypted using OpenPGP (IETF RFC 2440), or on a mutually agreed basis, PGP 2.6 or greater (using keys generated with the RSA algorithm). Free software implementations of the OpenPGP standard are available at <http://www.gnupg.org/>.

Firewall. A firewall should be deployed to protect HTTP servers.

CLIENT AND SERVER SPECIFICATIONS

Synchronization. Each Client and Server should be synchronized to a clock in the network of atomic clocks that is accessible via the Internet. The Client and Server should be synchronized as necessary to ensure synchronization with an atomic clock +/- 5 seconds. Please refer to Appendix A, 'Time Synchronization' for references on public sites for synchronization.

FOR EVALUATION PURPOSES ONLY

TESTING GUIDELINES

NAESB INTERNET ET TEST GUIDELINES

Implementation of Internet ET requires testing to assure all parties are prepared to operate according to the Internet ET. This document focuses on testing standards for establishing Internet ET connectivity with a trading partner. Testing for transaction and other Quadrant-specific testing standards can be found in each Quadrant's QEDM.

Internet ET Connectivity testing standards may include:

- Connectivity test scripts. These scripts define the steps needed to adequately test connectivity.
- Technical Exchange Worksheet (TEW). This worksheet defines important operations parameters for a trading partner. The parameters include Internet ET URL's, contacts and other information. See Appendix C for an example TEW.

Common Internet ET errors include:

- Misspelled keywords (e.g. 'content-type'), or spacing in a keyword
- Header 'content-type' missing
- MIME boundary not correct
- Malformed MIME segments
- Content-length does not match actual length
- PGP MIME malformed (found with some versions of PGP)

GENERAL TESTING ASSUMPTIONS

The following assumptions apply to Internet ET testing:

- This document covers Internet ET testing. Transactions and business process test plans can be found in the QEDM.
- Testing may uncover problems. Problems found during testing should be expected.
- Testing is a basic demonstration of competency, and may not uncover all problems that may eventually require correction.
- In normal circumstances, trading partner to trading partner Internet ET connectivity testing takes approximately two weeks.

TESTING GOALS

The primary testing goals of this Internet ET are:

- Establish Internet ET connectivity between trading partners including Internet connections and encryption compatibility.
- Validate Internet ET header formatting and delimiters
- Validate that normal production transaction files can be delivered.
- Validate that a large file (1MB or larger) can be delivered.
- Validate that Internet ET Receipts ('gisb-acknowledgement-receipt') are being delivered.
- Validate that protocol failures are handled properly.
- Validate that exchange failures are handled properly.

- Validate that encryption/decryption and digital signature failures are handled properly.

TEST EXECUTION

Test Scripts

Test scripts provide a step-by-step process for testing trading partner Internet ET connectivity. Test script scenarios test for both positive (accept) and negative (reject) results. Typical test scripts involve an exchange (Request and Response) of data between trading partners, with each TP confirming receipt of test file exchange via normal Internet ET standards. A copy of the payload file can be sent via e-mail for verification.

Test scripts can validate:

- That received files were not corrupted.
- Fail-over mechanisms by simulating a protocol failure and an exchange failure, triggering the appropriate notices to the TP contacts.
- Encryption failure processes by simulating an encryption/decryption failure, triggering the appropriate notices to the TP contacts.
- System time clock synchronization

Recommended Internal Tests

In addition to tests executed with trading partners, the following tests are recommended as internal tests of Internet ET systems.

- Acquire or develop an HTML page for interactive file upload (sample code is earlier in this document). Test the interactive file upload to your own server using an interactive browser.
- Stress Test. Ability to send and receive large production files (e.g. 10MB minimum uncompressed) and simultaneous usage. Simultaneous loading can be tested by requesting several other trading partners and/or several parties within your own company conduct Internet ET transfers concurrently.
- Fail-over Test. Test any processes triggered by a protocol or exchange failure by your trading partner.
- Invalid Userid/Passwords. Thoroughly test using the incorrect userid and password against the secure directory.
- Simulated Errors. Test various simulated errors in both file transfers and in OpenPGP or PGP decryption.

APPENDIX TABLE A – INTERNET ET STANDARD ERROR CODES AND MESSAGES

These errors and warnings are strictly related to problems found in the Receiving Program or decryption levels of processing before translation. Errors and warnings generated by the Client batch browser are assumed to be documented at the Client site to distinguish them from problems occurring in the Receiving Program or decryption. Numbering schemes and descriptions should aid in this distinction.

EEDM### standard error format with ### representing a numeric value; further processing will not take place

WEDM### standard warning format with ### representing a numeric value; further processing will take place

The string for the error or warning should appear in the following format:

[Validation Code];[Description];[supplemental message to be defined by the issuing site up to 80 characters]

Internet ET Standard Error Codes and Messages

Validation Code	Description	Data Element	Data Element Required or. Mutually Agreed
EEDM100	Missing 'from' Common Code Identifier code	from	required
EEDM101	Missing 'to' Common Code Identifier	to	required
EEDM102	Missing input format	input-format	required
EEDM103	Missing data file	input-data	required
EEDM104	Missing transaction set	transaction-set	mutually agreed
EEDM105	Invalid 'from' Common Code Identifier	from	required
EEDM106	Invalid 'to' Common Code Identifier	to	required
EEDM107	Invalid input format	input-format	required
EEDM108	Invalid transaction set	transaction-set	mutually agreed
EEDM109	No parameters supplied	parameter string	required
EEDM110	Invalid 'version'	version	required
EEDM111	Missing 'version'	version	required
EEDM112	'receipt-security-selection' not mutually agreed	receipt-security-selection	mutually agreed
EEDM113	Invalid 'receipt-security-selection'	receipt-security-selection	mutually agreed
EEDM114	Missing 'receipt-disposition-to'	receipt-disposition-to	required
EEDM115	Invalid 'receipt-disposition-to'	receipt-disposition-to	required
EEDM116	Missing 'receipt-report-type'	receipt-report-type	required
EEDM117	Invalid 'receipt-report-type'	receipt-report-type	required
EEDM118	Missing 'receipt-security-selection'	receipt-security-selection	mutually agreed
EEDM119	Mutually agreed element, refnum, not present	refnum	mutually agreed
EEDM601	Public key invalid	file itself	required - security
EEDM602	File not encrypted	file itself	required - security
EEDM603	Encrypted file truncated	file itself	required - security
EEDM604	Encrypted file not signed or signature not matched	file itself	required - security
EEDM699	Decryption Error		required for general decryption errors not specifically identified by OpenPGP or PGP messages or exit codes
EEDM701	Sending party not associated with Receiving party		required

NAESB RGQ & REQ Internet Electronic Transport Model Business Practices – RXQ.7

Validation Code	Description	Data Element	Data Element Required or. Mutually Agreed
EEDM702	Package file format not recognized by Receiving party		required when the file format is not recognized by the receiver (e.g. not expecting 855 or not expecting Flat-File or XML)
EEDM703	Data set exchange not established for Trading Partner		required if the translator does not handle this exception
EEDM999	System error		required for general system errors to indicate severe errors in processing at the receiving site
EEDM120	Mutually agreed element refnum-orig not present	refnum-orig	mutually agreed
EEDM121	Duplicate refnum received	refnum	mutually agreed
WEDM100	Transaction set sent not mutually agreed	transaction-set	mutually agreed
WEDM102	'receipt-security-selection' not mutually agreed	receipt-security-selection	mutually agreed
WEDM103	Missing 'receipt-security-selection'	receipt-security-selection	mutually agreed
WEDM104	Element refnum received, not mutually agreed; ignored	Refnum	mutually agreed
WEDM105	Refnum-orig received by not mutually agreed; ignored	refnum-orig	mutually agreed

APPENDIX A - Reference Guide

Receiving Program

Receiving Programs can be written using Active Server Pages (ASP), Common Gateway Interface (CGI), Java Server Pages (JSP), Java Servlet technology, PHP and other technologies.

Information on ASP may be found on Microsoft's web site (www.microsoft.com).

A source on CGI is a book entitled 'Special Edition Using CGI' by Jeffrey Dwight and Michael Erwin.

Information on JSP and Servlet technology may be found at SUN's web site (<http://java.sun.com>).

Firewall Security

A 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: (www.naesb.org) Primary reference for energy industry standards.

HTTP

The NAESB Internet ET architecture is based on HTTP 1.1, and all implementations should be compatible with this version. 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

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>

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>.

PGP Software

PGP is available for a variety of operating systems and platforms. For more information contact Network Associates (<http://www.nai.com>) or PGP Corporation (<http://www.pgp.com>)

Time Synchronization

Time synchronization is required to assure that all trading partners' transaction times are accurate. Testing has shown that the clocks on all computer systems drift. 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.

Each NAESB business process may have unique time-synchronization requirements. Refer to the QEDM for time-synchronization standards for target markets. Servers need to be time-synchronized according to the standards needed for the most-restrictive target market (i.e.

smallest drift allowance).

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.

An easy way to obtain the current time is from the U. S. Naval Observatory's Web site at 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, including IETF NTP, Internet daytime, nisttime / usnotime.

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

- <http://tycho.usno.navy.mil/ntp.html>
- <http://www.ccd.bnl.gov/xntp>

APPENDIX B – FREQUENTLY ASKED QUESTIONS

- Q1:** How many times do I attempt to send an Internet ET package unsuccessfully before I notify my partner?
- Q2:** Do I send my 'gisb-acknowledgement-receipt' before or after I decrypt the Internet ET package?
- Q3:** What cryptographic algorithms should we use or not use?
- Q4:** Use of 'time-c-qualifier' across quadrants. We understand that the retail quadrants require the 'time-c-qualifier' for 'gisb-acknowledgement-receipt', while the WGQ does not require this data element. If we participate in multiple quadrants, which standard do we use?
- Q5:** NAESB EDM / AS2 Compatibility. What is the status of NAESB compatibility with AS2?
- Q6:** Atomic Clock Synchronization. How often do we need to synchronize our system clocks with an atomic clock?
- Q7:** Internet Continuous Connection. As an end user, do I need a continuously-connected internet Web server to participate in the Internet EDM in the energy industry, or can I just use a dial-up connection to my ISP and my favorite shrink-wrapped browser software?
- Q8:** Use of ANSI X12.58. If we use ANSI X12.58 encryption do we still need to use OpenPGP or PGP encryption?
- Q9:** What does NAESB recommend for the OpenPGP/PGP descriptive text?

Q1: How many times do I attempt to send an Internet ET package unsuccessfully before I notify my partner?

A: The Internet ET 'exchange failure' standard requires that you attempt to send a package at least three times over a 30- to 120-minute period. At minimum, this means 30 minutes has elapsed between your first failed attempt and your third failed attempt. At maximum, 120 minutes has elapsed between your first failed attempt and your third failed attempt. You should not wait longer than 120 minutes between your first failed attempt and your last failed attempt to notify your trading partner.

For example, if you make your first attempt at time 00:00:00, and your third attempt at time 00:30:00, your second attempt can occur any time between the first and third. If the third attempt fails, you have an 'exchange failure' and should notify your trading partner.

Q2: Do I send my 'gisb-acknowledgement-receipt' before or after I decrypt the Internet ET package?

A: Either. If you decrypt packages after you have sent the 'gisb-acknowledgement-receipt', errors found must be communicated to your trading partners using the Error Notification transaction. You should indicate in your TEW when you will decrypt packages.

Regardless of when you decrypt, the 'time-c' timestamp does not change. It is always the time the last byte was received by the Server from the Sender.

Q3: What cryptographic algorithms should we use or not use?

A: OpenPGP implementations should use DSA and El Gamal, and PGP implementations should use RSA.

Q4: Use of 'time-c-qualifier' across quadrants. We understand that the retail quadrants require the 'time-c-qualifier' for 'gisb-acknowledgement-receipt', while the WGQ does not require this data element. If we participate in multiple quadrants, which standard do we use?

A: You are required to follow the quadrant standards that govern the transaction or business process. For example, if you are executing a WGQ nomination, then you should adhere to WGQ standards, which do not require the 'time-c-qualifier'. If you are executing an REQ enrollment, you need to adhere to the REQ standards, which require 'time-c-qualifier'. Of course, all parties can mutually-agree to use the 'time-c-qualifier'.

Q5: NAESB EDM / AS2 Compatibility. What is the status of NAESB compatibility with AS2?

A: AS2 and NAESB EDM are no longer compatible. The GISB/NAESB EDM and AS2 standards were separated as of version 12 of AS2. The AS2 standard now supports the UCC profile, and not the GISB profile. At this time NAESB is not pursuing an IETF standard for the Internet ET.

Q6: Atomic Clock Synchronization. How often do we need to synchronize our system clocks with an atomic clock?

A: Systems should be synchronized as often as necessary to maintain the required +/- 5 second variance with the NIST atomic clock. Some business processes may require more stringent synchronization. Refer to quadrant standards for time-synchronization standards of business processes.

Q7: Internet Continuous Connection. As an end user, do I need a continuously-connected internet Web server to participate in the Internet EDM in the energy industry, or can I just use a dial-up connection to my ISP and my favorite shrink-wrapped browser software?

A: An interactive browser connection is not enough to actively participate in the system. Internet ET requires a Server with a permanent Internet connection capable of receiving files without operator intervention. This Server may exist at a service provider.

Q8: Use of ANSI X12.58. If we use ANSI X12.58 encryption do we still need to use OpenPGP or PGP encryption?

A: Yes. The use of encryption such as X12.58 on payload files is outside the scope of the NAESB encryption standards.

Q9: What does NAESB recommend for the OpenPGP/PGP descriptive text?

A: There are no Internet ET standards for the information provided in the OpenPGP/PGP descriptive text data element. Implementers are encouraged to use their company name in this data element.

FOR EVALUATION PURPOSES ONLY

APPENDIX C – SAMPLE TECHNICAL EXCHANGE WORKSHEET (TEW)

Company and Contact Information

Company info:

Service Provider info (optional):

Contacts	Business Contact	Technical Contact
Primary Name:		
Telephone:		
Fax:		
E-mail:		
Secondary Name:		
Telephone:		
Fax:		
E-mail:		

Transport Specifications	Test	Production
DUNS/DUNS+4 Number		
HTTP 'to' Value		
HTTP 'from' Value		
Using 'time-c-qualifier' in Receipt? (Y/N)		
Decryption After Receipt/Using Error Notification Transaction (Yes/No)		
Primary Internet ET URL		
Server Name:		
CGI Path:		
Port:		
Userid:		
Password:		
PGP Public Key	Distribution	Distribution
Finger Print	Distributed with Key	Distributed with Key
Userid (Alpha, spaces, numbers only; no special characters)		

APPENDIX D - CROSS-REFERENCE BETWEEN INTERNET ET TRANSPORT AND WGQ EDM VERSION 1.7

‘***’ denotes that actual language of the WGQ EDM standard differs from the language of the Internet ET standard. This cross-reference was prepared in March of 2004. It is intended to be a resource to help implementers find sections from the old WGQ EDM in the new Internet ET standard.

Internet ET Standard	WGQ EDM Standard	Internet ET Standard Narrative
RXQ.0.1.1	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 energy transactions.
RXQ.0.1.2	0.1.2	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.
RXQ.0.3.1	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 DUNS Number at the Branch Location level; OR 2) to accommodate accounting for an entity that is identified at the Branch Location level.
RXQ.7.1.1	4.1.2.	The Internet Electronic Transport (ET) does not pick winners, rather it should create an environment where the marketplace can dictate a winner or winners
RXQ.7.1.2	4.1.3.	Internet ET solutions should be cost effective, simple and economical
RXQ.7.1.3	4.1.4.	Internet ET solutions should provide for a seamless marketplace for energy
RXQ.7.1.4	4.1.6.	Parties should interface with third-party vendors according to NAESB Internet ET standards
RXQ.7.1.5	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
RXQ.7.1.6	4.1.12.	Protocols and tools that parties elect to support should be ‘Internet-compatible’

Internet ET Standard	WGQ EDM Standard	Internet ET Standard Narrative
RXQ.7.1.7	4.1.14.	The industry should use standard policies and guidelines for testing
RXQ.7.1.8	4.1.15.	The NAESB Internet ET should not set standards for site-level security. Individual organization security standards should be relied upon
RXQ.7.1.9	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
RXQ.7.1.10	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
RXQ.0.2.56	4.2.20.	'Internet ET Testing'. Testing electronic packages between trading partners includes testing of: A) Connectivity; B) Encryption/Decryption; and C) Digital signatures where appropriate
RXQ.0.2.57	4.2.21**	'Fail-over' defines a prescribed process executed when a NAESB Internet ET Client fails to establish a connection to the target NAESB Internet ET Server
RXQ.0.2.58	4.2.22**	'Trading Partner' is a party that enters into an agreement with another party to transact business electronically using the Internet ET standard
RXQ.0.2.59	4.2.23**	'Originating party' is any party originating/creating the package. This could also include a third-party
RXQ.0.2.60	4.2.24**	'Third-Party' is any organization that a trading party uses to provide services to comply with the required elements of the Internet ET
RXQ.0.2.61	4.2.25**	'Receiving Party' is any party that hosts (either in-house or outsourced) an Internet ET compliant server capable of receiving Internet ET packages
RXQ.0.2.62	4.2.25**	'Receiving Program' is a program or set of programs that process HTTP Requests from a Sender. The Receiving Program is responsible for generating the 'gisb-acknowledge-receipt', which includes any party that hosts (either in-house or outsourced) an Internet ET compliant server capable of receiving Internet ET packages

Internet Standard	ET	WGQ EDM Standard	Internet ET Standard Narrative
RXQ.0.2.63		4.2.26**	'Trading Partner Agreement', or 'TPA' is a legal agreement between trading parties. The TPA often dictates service level agreements and problem remediation processes. The TPA may include technical exchange information such as URLs, et cetera
RXQ.7.3.1		4.3.1**	All parties sending and receiving data should accept a TCP/IP connection
RXQ.7.3.2		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
RXQ.7.3.3		4.3.7.	The designated Internet ET Server/Receiver site should be accessible via the public Internet. This does not preclude location of the designated site on a private intranet, as long as the designated site is also accessible via the public Internet
RXQ.7.3.4		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
RXQ.7.3.5		4.3.9.	A timestamp designates the time a file is received at the Receiver's designated site. The timestamp consists of the 'time-c' data element, and in some cases the 'time-c-qualifier' data element. Refer to QEDM standards for use of the 'time-c-qualifier'
RXQ.7.3.6		4.3.9	The Receiver generates a timestamp upon the successful receipt of a complete file. The timestamp should be generated by the Receiving Program immediately, prior to further processing by the Receiving Program.
RXQ.7.3.7		4.3.9	After timestamp generation, the Receiver sends an immediate HTTP Response to the Sender. The 'gisb-acknowledgement-receipt', which includes the timestamp data element(s), is the primary part of the HTTP Response.
RXQ.7.3.8		4.3.10**	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. Computer clocks should be synchronized as necessary to ensure at minimum +/- 5 second synchronization with an atomic clock. Specific business processes may have tighter synchronization requirements
RXQ.7.3.9		4.3.11**	The HTTP Response should be sent to the Internet Protocol (IP) address of the HTTP Request

Internet Standard	ET	WGQ EDM Standard	Internet ET Standard Narrative
RXQ.7.3.10		4.3.12.	At a minimum, 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
RXQ.7.3.11		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 (IETF RFC 1945)
RXQ.7.3.14		4.3.14	The Internet ET roles for Sender and Receiver are defined in the following table. The entire table defines a unit of work:
RXQ.7.3.15		4.3.15	Trading partners should implement all security features (privacy, secure authentication, integrity, and non-repudiation) using a file-based approach via a commercially-available implementation of: A) An OpenPGP product as defined by IETF RFC 2440, or B) On a mutually agreed basis, PGP version 2.6 or greater using the RSA algorithm to generate keys
RXQ.7.3.16		4.3.15	Trading partners should implement basic authentication.
RXQ.7.3.17		4.3.15	Encryption keys should be self-certified. The exchange of keys should be done in a secure manner such as via postal mail. Key policies, including key exchange policies should be communicated to trading partners.
RXQ.7.3.18		4.3.15	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.
RXQ.7.3.19		4.3.36.	Internet protocols should be used for accessing all industry business functions
RXQ.7.3.20		4.3.37.	Batch and Interactive Browsers should use Internet-compatible common browser software
RXQ.7.3.21		4.3.56**	Trading partners should use common codes for legal entities for the Internet ET 'to' and 'from' data elements

Internet ET Standard	WGQ EDM Standard	Internet ET Standard Narrative
RXQ.7.3.22	4.3.64.	Private network connections to NAESB Internet ET servers, which include all NAESB 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
RXQ.7.3.23	4.3.70**	Parties should be limited to the NAESB Internet ET approved list of available TCP ports for Internet ET implementations
RXQ.7.3.24	4.3.71, 4.1.37	Internet ET implementations should not require any inbound ports to be opened on the Sender's firewall.
RXQ.7.3.25	4.3.88.	Internet ET Servers should use 128-bit Secure Socket Layer (SSL) encryption
7.3.50	7.3.50	The question is whether individual implementations are free to use HTTP HEAD command, prior to using the POST command to deliver the NAESB payload. When implementing a NAESB Internet ET solution, the standard clearly relies on the HTTP protocol spec for details of how to implement the protocol. It is also clear that the HTTP POST command should be used, and not the GET command.

Version Notes

Version 1.0 NAESB REQ and RGQ Model Business Practices were published on September 27, 2005. The model business practices reflect REQ and RGQ Executive Committee Action on October 8, 2003, December 10, 2003, May 5, 2004, May 28, 2004, August 25, 2004, November 17, 2004, March 4, 2005, and August 24, 2004, and REQ and RGQ member ratification on November 24, 2003, March 1, 2004, June 28, 2004, October 7, 2004, December 30, 2004, May 13, 2005, August 30, 2005 and September 26, 2005.

Revised to include the minor corrections adopted by the Retail Executive Committees on May 10, 2006; Errata effective date: 07/14/2006.

Revised to include the minor correction adopted by the Retail Executive Committees on January 4, 2008; Errata effective date: 01/29/2008.

Appendix 1

RXQ.6.1 Electronic Data Interchange Trading Partner Agreement

The Electronic Data Interchange Trading Partner Agreement (EDI TPA) and the NAESB Trading Partner Agreement User's Guide for Use in Retail Applications are included in Appendix 1. An executable version of the EDI TPA is downloadable from the NAESB web site (<http://www.naesb.org>).

FOR EVALUATION PURPOSES ONLY

ELECTRONIC DATA INTERCHANGE
TRADING PARTNER AGREEMENT

THIS ELECTRONIC DATA INTERCHANGE TRADING PARTNER AGREEMENT (the "Agreement") is made as of _____, _____, by and between _____, a _____ [specify corporation or other entity type], with offices at _____ and _____, a _____, [specify corporation or other entity type] with offices at _____ (collectively, the "parties").

RECITALS

WHEREAS, the parties desire to facilitate transactions, reports and other information exchanged by electronically transmitting and receiving data in agreed formats; and

WHEREAS, the parties desire to assure that such transactions are not legally invalid or unenforceable as a result of the use of available electronic technologies for the mutual benefit of the parties; and

WHEREAS, the parties desire to enter into this Agreement to govern their relationship with respect to computer to computer exchange of information, also known as Electronic Data Interchange ("EDI") transactions; and

WHEREAS, recognizing that this Trading Partner Agreement (TPA) is a confidential document whose revelation could jeopardize the commerce and communication that is conducted between the parties to this agreement, the parties should take at least the same amount of care to secure this TPA as would be taken with any other proprietary, internal or contractual document.

NOW THEREFORE, in consideration of the premises and covenants herein contained, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties, intending to be legally bound, hereby agree as follows:

Section 1. Prerequisites

1.1 Data Communications. Each party may electronically transmit to or receive from the other party any of the transaction sets (collectively "Documents") listed in the Exhibit(s), as such Exhibit(s) may be revised by written agreement. Any transmission of data which is not a Document, a Functional Acknowledgement, an electronic delivery mechanism error notification, or a time-stamp receipt response or record (collectively "Data Communications") shall have no force or effect between the parties. All Data Communications shall be transmitted in accordance with the standards and the published industry guidelines set forth in the Exhibit(s). The Exhibit(s) to this Agreement is(are) attached hereto. Any modification of the provisions contained in the body of this Agreement will be effective as set forth in the Exhibit(s).

1.2. Third Party Service Providers

1.2.1 Data Communications will be transmitted electronically to each party as specified in the Exhibit(s), either directly or through any third party service provider ("Provider") with whom either party may contract. Either party may modify its election to use, not use or change a Provider upon 30 days prior written notice to the other party.

1.2.2 Each party shall be responsible for the costs of any Provider with whom it contracts, unless otherwise set forth in the Exhibit(s). Each party shall be responsible for services and performance needed to carry out its responsibilities under this agreement.

1.2.3 Notwithstanding the acts or omissions of its Provider, for purposes of this Agreement, each party is responsible for transmitting, receiving, storing or handling Data Communications to the extent required to effectuate transactions pursuant to Section 2.

1.3 System Operations. Each party, at its own expense, shall provide and maintain the equipment, software, services and testing necessary to transmit Data Communications to, and receive Data Communications from the parties' respective Receipt Computers.

1.4 Security Procedures

1.4.1 Each party shall use those security procedures specified in the North American Energy Standards Board ("NAESB") standards and the Exhibit(s). The manner in which public encryption keys are to be changed and/or exchanged will be specified in the Exhibit(s).

1.4.2 Security Key Exchanges. The parties shall maintain a public key used to facilitate secure electronic communication. The parties shall change their public key as set forth in the Exhibit(s). However, in emergency situations in which it is necessary to change a key immediately, each party shall provide the other party with immediate notice of the change. Each party shall provide to the other its public key by either: (a) a certified or receipt mail service using a diskette with the public key contained in an ASCII text file; or, (b) an electronic simple mail transfer protocol ("SMTP") mail message with the public key contained in the body. The public key shall be verified by the party to whom it is sent by validating the fingerprint of the public key by phone or by other comparable means.

1.5 Signatures. Each party shall adopt as its signature private keys which shall be applied to each document transmitted by such party ("Digital Signature "). Such Digital Signature, when decrypted by the receiving party, will be used to authenticate the identity of the sender.

Section 2. Transmissions

2.1 Proper Receipt

2.1.1 The "Receipt Computer" shall be defined in the Exhibit(s) as the receiving party's Uniform Resource Locator ("URL"), which describes the protocols which are needed to access the resources and point to the appropriate Internet locations. Where the parties employ the services of Providers to transmit and receive Documents, the Receipt Computer shall be defined in the Exhibit(s) as the receiving party's URL provided by the receiving party's Provider.

2.1.2 Documents shall not be deemed to have been properly received, and no Document shall give rise to any obligation, until accessible to the receiving party at such party's Receipt Computer designated in the Exhibit(s), as evidenced by the receipt by sending party of the HTTP response initiated by receiving party. The HTTP response shall specify the date and time of receipt of a Document at the receiving Internet server (also called "time-c"). No Document shall have any effect if the HTTP response is not received by sending party, or if the HTTP response indicates an error.

2.2 Digital Signature Verification and Decryption. Upon proper receipt of any Document, the receiving party shall attempt to decrypt the Document and verify the digital signature of the sending party. If the Document is verified and the decryption is successful, the receiving party shall transmit a Functional Acknowledgment in return. If the Document is verified and the decryption is unsuccessful, the receiving party shall send the applicable error message to the

sending party. The sending party shall attempt to correct the error and promptly retransmit the Document or otherwise contact the receiving party.

2.3 Functional Acknowledgement and Response Document

2.3.1 For the purposes of this Agreement, a "Functional Acknowledgment" means an ASC X12 Transaction Set 997 which confirms a Document has been received and whether all required portions of the Document are syntactically correct or not, but which does not confirm the substantive content(s) of the related Document.

2.3.2 If the Functional Acknowledgment indicates an error, neither party shall rely on the Document. The sending party shall attempt to correct the error and promptly retransmit the Document or otherwise contact the receiving party. If the Functional Acknowledgment does not indicate any error, the Functional Acknowledgment shall constitute conclusive evidence a Document has been received in syntactically correct form.

2.3.3 If there has been proper receipt pursuant to Section 2.1, verification and successful decryption pursuant to Section 2.2, and if the receiving party nevertheless fails to transmit a Functional Acknowledgment, the sending party's records of the contents of the Document shall control, unless the sending party has retransmitted a Document pursuant to Section 2.3.7.

2.3.4 By mutual agreement, the parties may designate in the Exhibit(s) a "Response Document" Transaction Set as a substitute for or in addition to an ASC X12 Transaction Set 997. A Response Document confirms that a Document has been received, and whether all required portions of the Document are syntactically correct, and contains data sent by the receiving party to the sending party in response to the substantive content of the related Document.

2.3.5 If the Response Document indicates an error, neither party shall rely on the Document or portion of the Document which is in error, if known. The sending party shall attempt to correct the errors and promptly retransmit the Document or applicable portion or otherwise contact the receiving party. If the Response Document does not indicate any error, the Response Document shall constitute conclusive evidence a Document has been received in syntactically correct form.

2.3.6 If the parties have mutually agreed to the use of a Response Document, and if there has been proper receipt pursuant to Section 2.1, verification and successful decryption pursuant to Section 2.2, and if the receiving party nevertheless fails to transmit a Response Document, the sending party's records of the contents of the Document shall control unless the sending party has retransmitted a Document pursuant to Section 2.3.7.

2.3.7 Retransmissions. If the sending party of a Document has not received a corresponding Functional Acknowledgment or Response Document within the time frame indicated in the Exhibit(s), the sending party shall retransmit the Document and such Document shall be considered a new transmission for purposes of Section 2.

Section 3. Terms

3.1 Transaction Terms and Conditions. This Agreement is intended to facilitate Data Communications between the parties concerning the transactions related to transportation or sales conducted pursuant to underlying written agreements. In the event of conflict between

this Agreement and the subject underlying written agreement(s), the terms and conditions of the underlying agreement(s) shall control.

3.2 Terms and Conditions of Reports and Other Information. In the absence of any other written agreement applicable to reports and other information transmitted pursuant to this Agreement, such reports and other information shall be subject to:

[A] those terms and conditions, including any terms for payment, included in the Exhibit(s);
and

[B] such additional terms and conditions as may be determined in accordance with applicable law.

3.3 Change in Terms and Conditions. Notwithstanding Section 4.1 of this Agreement, if any party determines that Data Communications under this Agreement are altered by a subsequent change to a party's tariff or obligation imposed by a governmental entity exercising jurisdiction over that party, then the affected party shall give immediate notice defining which Data Communications under this Agreement are affected, and the reasons therefore, and may provide notice of termination of this Agreement as provided in Section 4.8, effective immediately upon receipt of such notice by the other party to this Agreement.

3.4. Confidentiality. No information contained in any Document or otherwise exchanged between the parties shall be considered confidential, except to the extent provided in Section 1.5 or in the Exhibit(s), by written agreement between the parties, or by applicable law.

3.5. Validity: Enforceability

3.5.1 This Agreement has been executed by the parties to evidence their mutual intent to be bound by the terms and conditions set forth herein relating to the electronic transmission and receipt of Data Communications.

3.5.2 Any Document properly transmitted pursuant to this Agreement shall be considered, in connection with any transaction, any other written agreement described in Section 3.1, or this Agreement, to be a "writing" or "in writing"; and any such Document when containing, or to which there is applied, a Digital Signature ("Signed Documents") shall be deemed for all purposes (a) to have been "signed" and (b) to constitute an "original" when printed from electronic files or records established and maintained in the normal course of business.

3.5.3 The parties agree not to contest the validity or enforceability of Signed Documents under the provisions of any applicable law relating to whether certain agreements are to be in writing or signed by the parties to be bound thereby. Signed Documents, if introduced as evidence on paper in any judicial, arbitration, mediation or administrative proceedings, will be admissible as between the parties to the same extent and under the same conditions as other business records originated and maintained in documentary form. Neither party shall contest the admissibility of copies of Signed Documents under either the business records exception to the hearsay rule or the best evidence rule on the basis that the Signed Documents were not originated or maintained in documentary form.

Section 4. Miscellaneous

4.1 Term. This Agreement shall be effective as of the date first set forth above and shall remain in effect until terminated by either party with not less than 30 days prior written notice

specifying the effective date of termination; provided, however, that written notice for purposes of this paragraph shall not include notice provided pursuant to an EDI transaction; further provided, however, that any termination shall not affect the respective obligations or rights of the parties arising under any Documents or otherwise under this Agreement prior to the effective date of termination.

4.2 Severability. Any provision of this Agreement which is determined by any court or regulatory body having jurisdiction over this Agreement to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this Agreement or affecting the validity or enforceability of such remaining provisions.

4.3 Entire Agreement. This Agreement and the Exhibit(s) constitute the complete agreement of the parties relating to the matters specified in this Agreement and supersede all prior representations or agreements, whether oral or written, with respect to such matters. No oral modification or waiver of any of the provisions of this agreement shall be binding on either party. No obligation to enter into any transaction is to be implied from the execution or delivery of this Agreement.

4.4 No Third Party Beneficiaries. This Agreement is solely for the benefit of, and shall be binding solely upon, the parties, their agents and their respective successors and permitted assigns. This Agreement is not intended to benefit and shall not be for the benefit of any party other than the parties hereto and no other party shall have any right, claim or action as a result of this Agreement.

4.5 Governing Law. This Agreement shall be governed by and interpreted in accordance with the laws of _____ [specify state, commonwealth, province, etc.] of _____, excluding any conflict-of-law rules and principles of that jurisdiction which would result in reference to the laws or law rules of another jurisdiction.

4.6 Force Majeure. No party shall be liable for any failure to perform its obligations in connection with any transaction or any Document, where such failure results from any act of God or other cause beyond such party's reasonable control (including, without limitation, any mechanical, electronic or communications failure) which prevents such party from transmitting or receiving any Documents and which, by the exercise of due diligence, such party is unable to prevent or overcome.

4.7 Exclusion of Certain Damages. Neither party shall be liable to the other for any special, incidental, exemplary or consequential damages arising from or as a result of any delay, omission or error in the electronic transmission or receipt of any Data Communications pursuant to this Agreement, even if either party has been advised of the possibility of such damages and REGARDLESS OF FAULT. Any limitation on direct damages to software and hardware arising from Data Communications under this Agreement shall be set forth in the Exhibit(s).

4.8 Notices. All notices required or permitted to be given with respect to this Agreement shall be given by mailing the same postage prepaid, or given by fax or by courier, or by other methods specified in the Exhibit(s) to the addressee party at such party's address as set forth in the Exhibit(s). Either party may change its address for the purpose of notice hereunder by giving the other party no less than five (5) days prior written notice of such new address in accordance with the preceding provisions.

4.9 Assignment. This Agreement may not be assigned or transferred by either party without the prior written approval of the other party, which approval shall not be unreasonably withheld;

provided, any assignment or transfer, whether by merger or otherwise, to a party's affiliate or successor in interest shall be permitted without prior consent if such party assumes this Agreement.

4.10 Waivers. No forbearance by any party to require performance of any provisions of this Agreement shall constitute or be deemed a waiver of such provision or the right thereafter to enforce it.

4.11 Counterparts. This Agreement may be executed in any number of original counterparts all of which shall constitute one and the same instrument.

4.12 Reference Glossary. This section lists each defined term in this Agreement and cross references that term to its definition in the Agreement.

DEFINED TERM	WHERE DEFINED
Agreement	Header
Data Communications	Section 1.1
Digital Signature	Section 1.5
Documents	Section 1.1
Electronic Data Interchange, EDI	Recital
Functional Acknowledgment parties	Section 2.3.1
Provider	Header
Receipt Computer	Section 1.2.1
Response Document	Section 2.1.2
Signed Documents	Section 2.1.2
time-c	Section 2.3.4
Uniform Resource Locator, URL	Section 3.5.2
	Section 2.1.1
	Section 2.1.2

Each party has caused this Agreement to be properly executed on its behalf as of the date first above written.

Company Name: _____	Company Name: _____
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____

EXHIBIT ____

ELECTRONIC DATA INTERCHANGE TRADING PARTNER AGREEMENT

DATED _____

TO BE EFFECTIVE _____ (date)

1. Contact Information:
- Company Name: _____
- Street Address: _____
- City: _____
- State/Province/Commonwealth: _____
- Zip/Postal Code: _____
- Attention [Name, Title]: _____
- Phone: _____ Fax: _____ Email Address: _____
- Legal Entity Common Code (D-U-N-S®(Number): _____
-
- Company Name: _____
- Street Address: _____
- City: _____
- State/Province/Commonwealth: _____
- Zip/Postal Code: _____
- Attention [Name, Title]: _____
- Phone: _____ Fax: _____ Email Address: _____
- Legal Entity Common Code (D-U-N-S®(Number): _____
-
2. Special Allocation Costs if Any: _____

(A registered trademark of Dun & Bradstreet Corporation)

EXHIBIT ____

ELECTRONIC DATA INTERCHANGE TRADING PARTNER AGREEMENT

DATED _____
TO BE EFFECTIVE _____ (date)

3. Communication Specifics:
- Company Name: _____
EDI Contact Phone Number: _____
Provider Name: _____
Receipt Computer URL (include host name or IP address, any non standard port, directory and program name as necessary): _____
Basic Authentication Userid: _____
Basic Authentication Password: _____
HTTP to/from Tag: _____
Is the "transaction set" supported in the HTTP envelope (Yes/No)? _____
- Company Name: _____
EDI Contact Phone Number: _____
Provider Name: _____
Receipt Computer URL (include host name or IP address, any non standard port, directory and program name as necessary): _____
Basic Authentication Userid: _____
Basic Authentication Password: _____
HTTP to/from Tag: _____
Is the "transaction set" supported in the HTTP envelope (Yes/No)? _____

[Parties should execute a separate Exhibit for each different URL.]

EXHIBIT ____

ELECTRONIC DATA INTERCHANGE TRADING PARTNER AGREEMENT

DATED _____
TO BE EFFECTIVE _____ (date)

5. Standards and Industry Guidelines: (Specify all applicable standards, issuing organizations, and published industry guidelines.)

Selected standards include, as applicable, all data dictionaries, segment dictionaries and transmission controls referenced in those standards for the transaction(s) contained in this Exhibit(s). The mutually agreed provisions of this Exhibit(s) shall control in the event of any conflict with any listed industry guidelines.

6. Security Procedures: (Define security procedures, including but not limited to encryption, authentication, and GPG or PGP version.)

6.1 Public Encryption Key Exchange Procedures:

a) Contact for public encryption key exchange (emergency and scheduled)

b) Method of contact and related information (phone number and/or e-mail address)

c) Chosen electronic method of key exchange

d) Scheduled public encryption key exchange procedures including frequency

e) Emergency public encryption key exchange procedures

f) Verification procedures to confirm appropriate exchange of public encryption keys

g) Other

EXHIBIT ____

ELECTRONIC DATA INTERCHANGE TRADING PARTNER AGREEMENT

DATED _____
TO BE EFFECTIVE _____ (date)

7. Terms and Conditions: (If no special terms and conditions have been agreed upon, enter "None.")

8. Data Retention: (If no special data retention procedures have been agreed upon, enter "None.")

9. Limitation on Direct Damages: (If no limitation has been agreed upon, enter "None.")

10. Confidential Information: (See Section 3.4. If no limitation has been agreed upon, enter "None.")

The undersigned do hereby execute this Exhibit pursuant to the Agreement attached and do hereby ratify said Agreement for all purposes set forth in this Exhibit.

Company Name: _____ Company Name: _____

By: _____ By: _____

Printed Name: _____ Printed Name: _____

Title: _____ Title: _____

**NAESB Trading Partner Agreement User's Guide
for Use in Retail Applications**

The purpose of this User's Guide is to explain how some common concerns related to using the NAESB Trading Partner Agreement (TPA) in a retail environment may be addressed. This is not meant to provide detailed instructions on completing each section of the agreement. The TPA, which has been in use for WGQ Applications since 1997, provides standard language that can be used as a starting point. The Exhibit to the TPA (Exhibit) provides contractual flexibility designed to address the unique circumstances between any two trading partners.

1. Why would I want to use the NAESB Trading Partner Agreement in a retail environment?

Originally developed for wholesale natural gas trading partners, the NAESB TPA has stood the test of time and has already been used in some retail markets with virtually no modification. The current version incorporates some new aspects that tailor it to retail. Its construction allows it to be customized as needed by the potential trading partners without diluting its value as a standardized agreement.

2. Does the term "EDI" refer exclusively to ASC X12 or can it be interpreted more broadly, i.e. covering all uniform electronic transactions?

As used in the NAESB TPA, "EDI" is used in its broadest¹ interpretation and refers to any electronic (computer to computer) transfer of data between the trading partners. If necessary, Section 7 of the Exhibit can be used to further define the term "EDI" as used by the trading partners.

3. The recitals at the beginning of the TPA state that the agreement is confidential, but Section 3.4 goes on to state that the content of the transactions covered by the agreement are not. Isn't this a conflict and since retail customer data is confidential, does this make it impossible to use the TPA for retail transactions?

There is no conflict. Section 3.4 was written conservatively by requiring the parties to itemize the information that they desire to be treated as confidential. The trading partners do this by itemizing the confidential data items in Section 10 of the Exhibit.

4. The datasets I use are not NAESB datasets but are very similar. Further, state regulations mandate their usage in my jurisdiction. Can the TPA accommodate this situation?

Sections 4 and 5 of the Exhibit facilitate customizing the TPA to any jurisdiction or accommodating any special needs the trading partners have. Section 4 of the Exhibit is a template where the specific transactions used by the parties can be listed within the table. Section 5 of the Exhibit can be used to reference datasets or transactions mandated for use in a specific jurisdiction.

5. Section 2 of the Exhibit provides for identification of Special Allocation Costs. What are these costs?

This is a general section where the parties may agree as to the cost recovery for any costs associated with transactions governed by the TPA. For example, in some jurisdictions, VAN fees are assessed when a party is unable to utilize the internet on a temporary basis.

¹ While the term EDI for the Wholesale Gas application refers to the ASC X12, such interpretation does not preclude broader usage.

**NAESB Trading Partner Agreement User's Guide
for Use in Retail Applications**

6. May I modify the TPA?

The use of the Exhibit allows trading partners to utilize the TPA in a wide variety of situations-without modifying the standard contract itself. If the trading partners modify the contract itself, this means the TPA is no longer the standard NAESB TPA and, at a minimum, the NAESB watermark must be removed from the document. In addition, any modification to the TPA terms, whether electronically or to the paper form, should be clearly communicated to all counterparties.

7. How do I customize the TPA to meet my specific needs?

The Exhibit provides an exhaustive template for filling in the needed implementation details to completely describe the trading partner's specific intentions.

8. The TPA contains no language about resolving disputes between the parties. Can dispute resolution language be added to the TPA?

The drafters of the NAESB TPA presumed that other Governing Documents, such as a master agreement between the trading partners or specific rules within a given jurisdiction, would dictate a dispute resolution procedure. If needed, dispute resolution language or a reference to a state's dispute resolution procedures could be added to Section 7 of the Exhibit.

9. The TPA does not address data back-up, yet it is a good practice and in many cases required by various federal and state requirements. Why doesn't the TPA address back-up?

The TPA is designed to address the transfer of information between trading partners and not any back-office systems issues including, but not limited to, data back-up. This, however, does not preclude two mutually agreeing parties from adding special terms and conditions addressing data back-up in Section 7 of the Exhibit.

10. Why is there no *course of dealing* and/or *course of performance* language in the TPA? If I want to add such language, how would I go about doing so?

The interpretation of *course of dealing* and *course of performance* varies from jurisdiction to jurisdiction. It would be difficult to agree on standard language to be included in a section covering this topic. However, this does not preclude two parties from adding such language in jurisdictions where it may be required or desired. This may require reviewing language in Sections 4.3 and 4.10 to determine if any modifications are necessary to address language that might be interpreted to preclude the addition of *course of dealing* and *course of performance* language. Following this review, parties can then agree to modify or supplement the language in Sections 4.3 or 4.10 by placing appropriate language in Section 7 of the Exhibit.

11. I just received the NAESB TPA from someone and it does not have the NAESB watermark on it - why?

There are several reasons this could happen. The company preparing the TPA may have deleted the NAESB watermark because they modified the TPA - or - the company preparing the TPA may have had word processor problems that prevented them from printing the watermark. Ask the company that sent you the TPA.

**NAESB Trading Partner Agreement User's Guide
for Use in Retail Applications**

12. How do I know if the TPA that someone sends me is the standard TPA?

There are several things you should check. Compare the TPA to the original you downloaded or received from NAESB. Make sure the date is the same, the watermark appears and that the copyright language is in place. Ask the company that forwarded the TPA to you.

13. Why is the watermark not appearing on the TPA that I downloaded from NAESB?

In the conversion process for word processors, there are differing ways that watermarks are dealt with. Make sure that you are reading the file you downloaded with the word processor for which it was formatted.

14. Why are the pages printing differently than the standard TPA as posted on the NAESB website?

Many word processors reformat documents according to the printer that you are using. When you initiate the TPA in your word processor, you may have to make some minor adjustments to the margins or font sizes to get the pagination to stay the same.

FOR EVALUATION PURPOSES ONLY



For information on membership in the
North American Energy Standards Board
contact the NAESB office at:
1301 Fannin, Suite 2350
Houston, Texas 77002
(713) 356-0060
(713) 356-0067 Fax
E-mail: naesb@naesb.org
www.naesb.org

Additional copies may be obtained from NAESB.