**NAESB Specification for Data Privacy Governing Third Party Access**

1. INTRODUCTION

1.1 About this Document

This document provides the technical and managerial details that a Third Party must demonstrate that it meets in its Certification Practice Statement. The following requirements are intended to support the NAESB REQ Model Business Practice Standards for Third Party Access to Smart Meter-based Information.

1. Definitions

2.1 Applicable Regulatory Authority is defined as 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 Customers through regulations and orders.

2.2 Authorization is defined as the result of the process by which the Retail Customer provides informed consent in a manner consistent with the applicable Governing Documents and any requirements of the Applicable Regulatory Authority.

2.3 Governing Documents is described as documents that determine the interactions among parties, including but not limited to: applicable law, regulatory documents (e.g. tariffs, rules, regulations), contractual agreements, Distribution Company Operational Manuals, and other relevant models and operational procedures.

2.4 Retail Customer is defined as any Entity that takes or is applying to take gas and/or electric services for its own consumption.

2.5 Smart Meter-based Information is defined as information and data from a smart meter identifiable to an individual Retail Customer, as defined and governed by the Governing Documents and which may be made available pursuant to the Governing Documents consistent with any requirements of the Applicable Regulatory Authority.

2.6 Third Party is defined as an entity that is permitted to receive Smart Meter-based Information in accordance with applicable law, regulation, the Governing Documents, and any requirements of the Applicable Regulatory Authority, other than: the Distribution Company and its contracted agents, the Applicable Regulatory Authority, ISOs or other regional entities, which seeks or is provided Smart Meter-based Information, including any Entity under contract with the Third Party to perform the services or provide the products as described in the Retail Customer’s Authorization.

1. Certification Practice Statement

A Third Party must submit a Certification Practice Statement which shall demonstrate and describe how its practices meet the following requirements and to which the Third Party shall certify the accuracy of the representations contained in the Certification Practice Statement.

3.1 Management and Accountability Requirements

3.1.1 A Third Party must verify the existence of internal documented information security and privacy policies and practices related to Smart Meter-based Information and identify the personnel responsible for ensuring the internal policies and practices are followed.

3.1.2 A Third Party must provide documentation to evidence training and ongoing awareness activities regarding their privacy policies and practices.

3.1.3 A Third Party must describe the internal auditing and monitoring practices for the collection, access, use, retention, and disclosure of Smart Meter-based Information activities.

3.1.4 A Third Party must maintain records related to their disclosures of Smart Meter-based Information to other Third Parties and retain those records for a reasonable period subject to the Governing Documents and requirements of the Applicable Regulatory Authority.

3.2 Notice and Purpose Requirements

3.2.1 A Third Party must demonstrate that its information privacy policies, including Authorization terms and conditions, related to Smart Meter-based Information are clear, concise, understandable, and accessible.

3.2.2 A Third Party must demonstrate that it has provided a reasonably conspicuous and clear notice to Retail Customers that their Smart Meter-based Information will not be received, used, retained, or disclosed to additional Third Parties without authorization by the Retail Customer.

3.2.3 A Third Party must certify that a Retail Customer’s Smart Meter-based Information be limited to only that information necessary to fulfill the purpose as set forth in the Retail Customer’s Authorization.

3.2.4 A Third Party must certify that a Retail Customer’s Smart Meter-based Information will only be used for the purpose(s) specified in the Retail Customer’s Authorization.

 3.3 Choice and Consent Requirements

3.3.1 A Third Party must describe practices to prevent unauthorized disclosure of Smart Meter-based Information to additional Third Parties.

3.3.2 A disclosing Third Party must describe its process for obtaining or confirming the Retail Customer’s Authorization to allow disclosure of the Retail Customer’s Smart Meter-based Information to additional Third Parties. The process should conform to the requirements in REQ.22.3.3.2.1.2 and REQ.22.3.3.2.1.3.

3.3.3 A Third Party must document the manner through which the Retail Customer may withdraw its Authorization for a Third Party to access Smart Meter-based Information.

3.3.4 If applicable, a Third Party must verify the form for obtaining Authorization from a Retail Customer specifies the terms and conditions of the Authorization.

3.4 Use and Retention Requirements

3.4.1. A Third Party must demonstrate that Smart Meter-based Information is being retained consistent with the requirements in REQ.22.3.5.1.1.

3.4.2. A Third Party must describe its procedure for ensuring the destruction of a Retail Customer’s Smart Meter-based Information for the following circumstances:

* The Retail Customer withdraws its Authorization
* The Smart Meter-based Information is no longer needed to fulfill the Authorized purpose
* The Retail Customer’s Authorization has reached the end of the specified period set forth in the Authorization
* As required by the Governing Documents or Applicable Regulatory Authority

3.5 Retail Customer Access Requirements

 3.5.1 A Third Party must describe the process by which a Retail Customer may obtain access to the Retail Customer’s Smart Meter-based Information. This process must be consistent with REQ.22.3.6.2.1.

 3.5.2 A Third Party must describe the process by which a Retail Customer may request that the Smart Meter-based Information be corrected where inaccuracies exist. This process must be consistent with REQ.22.3.6.2.1.

 3.5.3 A Third Party must describe its complaint process for the Retail Customer to address disputes. The complaint process must comply with the requirements in REQ.22.3.10.2.2.

3.6 Security and Safeguard Practices Requirements

 3.6.1 A Third Party must verify the existence of information privacy protections that protect Smart Meter-based Information under its control from loss, theft, unauthorized access or disclosure, unauthorized copying, misuse, or modification.

 3.6.2 A Third Party must describe their development of Privacy Use Cases created and/or reviewed for the development and updating of their privacy protection policies and practices. The Privacy Use Cases must comply with the requirements in REQ.22.3.8.2.1.3.

 3.6.3 A Third Party must certify they are performing periodic risk analyses to assess their privacy protection policies and practices related to the receipt, collection, management, use, retention, and disclosure of Smart Meter-based Information. A Third Party must provide a high-level description of how the analyses are conducted.

 3.6.4 A Third Party must describe policies that will trigger a mandatory risk analysis to be performed when one or more of the following conditions are met:

* Major changes occur within the organization that impact the Third Party’s data privacy practices related to the receipt, collection, management, use, retention, or disclosure of Smart Meter-based Information;
* Relevant, new applicable laws and/or regulations become effective; or
* An event occurs related to the Third Party’s unauthorized disclosure of Smart Meter-based Information.

3.6.5 A Third Party must provide documentation of the process to restore integrity of the system and data in the event of any breach of security of a system, under the Third Party’s control, that results in the unauthorized disclosure of Smart Meter-based Information.