Posting on NAESB Web Site

March 11, 2013

**RE: NAESB Wholesale Natural Gas Market Cybersecurity Standards Fact Sheet**

To provide additional information on the purpose and use of the NAESB cybersecurity standards related to the wholesale natural gas market, this fact sheet includes; a brief description of our wholesale natural gas market cybersecurity related standards, the purpose of the standards, the transactions to which they apply, and their use by specific wholesale natural gas market segments. There is also a brief discussion on regulatory implications, future developments and how these standards interact with the NAESB cybersecurity standards for the wholesale electric market. We hope you will find this fact sheet helpful. We understand that the standards, by their nature, are technical. However, it is important that decision-makers, who may not be well versed in the technical aspects of cybersecurity, have an opportunity to understand the benefits of implementing these cybersecurity standards and the protections and benefits they provide to the market.

**Description and purpose of the NAESB cybersecurity standards applicable to the wholesale natural gas market**

NAESB has developed wholesale natural gas market cybersecurity standards that support mutual entity authentication through the use of digital signatures, self-certification, and provision for public-private keys to access and protect market information and execute transactions, thus supporting an infrastructure of secure electronic communications.

The NAESB wholesale natural gas cybersecurity standards that support Electronic Data Interchange (EDI)-based transactions utilize PGP (Pretty Good Privacy), a process that encrypts and decrypts transactional data and is also used to create encrypted digital signatures. PGP provides: (1) confidentiality: the assurance that no one can read a transaction except the intended receiver(s), (2) authentication: the assurance that an entity is who it claims to be, (3) integrity: the assurance that data has not been altered (intentionally or unintentionally) from sender to recipient and from time of transmission to time of receipt, and (4) technical non-repudiation: that a party cannot deny having engaged in the transaction or having sent the electronic message.

PGP employs public-private key pairs, and the NAESB cybersecurity standards rely upon PGP as defined by IETF RFC 2440 protocol, or if parties mutually agree, PGP version 2.6 or greater using the RSA algorithm to generate the key pairs. The trading partners using PGP are self-certified and key policies, including polices for exchanges are communicated between trading partners. The lifecycle of the encryption keys is suggested to be no more than one year, and is determined by the key’s owner. The key exchange procedures are identified in NAESB’s Trading Partner Agreement document, (NAESB WGQ Standard 6.3.3).

For transactions utilizing Internet web sites, servers, and browsers, 128-bit Secure Socket Layer encryption (SSL) is used to secure the transport of electronic information between trading partners. The public and private keys (asymmetric) are used to create the symmetric session key. The session key is used to encrypt all transmitted data, thus providing protection and not adversely impacting transaction speed. In addition access to the underlying data is protected by user login and password requirements.

**Application of the NAESB cybersecurity standards in the wholesale natural gas market**

NAESB’s long-standing support for open standards has created a competitive marketplace of interoperable e-commerce products to serve the energy industry. As with other NAESB business practice standards initiatives, the cybersecurity related standards are intended to facilitate a wide array of implementations utilizing either in-house or third party software systems.

The NAESB wholesale natural gas cybersecurity standards facilitate an infrastructure of secure electronic communications under which the electronic transmission of data via EDI or browser based transactions is protected. There are more than fifty separate transactions identified for nominations, confirmations, scheduling of natural gas; flowing gas transactions including measurement, allocations, and imbalances; invoicing related transactions including invoices, remittances, statement of account; and capacity release transactions. The cybersecurity standards apply to interstate transmission providers, their customers and stakeholders who are parties to the transactions noted above. As other electronic transactions in the wholesale natural gas market are determined to require such electronic protection, they too can be included as applicable.

**Regulatory Implications of the NAESB cybersecurity standards**

The cybersecurity standards were developed to align with industry best practices and the most recent version (Version 2.0) of the standards were provided to the Federal Energy Regulatory Commission (FERC) as part of Docket No. 96-1-037, on March 4, 2011. On July 19, 2012, FERC, through incorporation by reference, adopted the standards and as such they are mandatory for entities that are jurisdictional under the Natural Gas Act. These standards, as is true for all NAESB standards, are reviewed against current market requirements, and are provided to FERC as they are updated.

**Future Developments for the NAESB cybersecurity standards**

There is a standing development item in the NAESB WGQ Annual Plan that specifically tasks NAESB with updating the wholesale natural gas cybersecurity standards based on advances in technology, markets and cyber threats. We are aware that there are updated version of the IETF protocols[[1]](#footnote-1) used for PGP, notably, IETF RFC 4880, and the cybersecurity industry is moving towards use of TLS[[2]](#footnote-2) rather than SSL, all of which may be considered by NAESB as the wholesale natural gas cybersecurity standards are reviewed. Additionally, NAESB receives requests for standards development throughout the year from industry participants.

Also the NAESB wholesale natural gas cybersecurity standards have been reviewed on two occasions by Sandia National Laboratories (SNL) on behalf of the Department of Energy (DoE). Each assessment worked much like an audit, where the standards were reviewed, observations made, and findings along with recommended actions provided. The recommended actions focused on cybersecurity, scalability, performance, data and transactional integrity, and confidentiality. The assessments also provided critical success factors and metrics of importance that would support the organization going forward as new standards were developed and existing standards were modified. In response to each assessment, NAESB has implemented numerous changes and refinements to the standards There have recently been dialogs regarding a third SNL security assessment of NAESB’s technical standards. These independent surety assessments by the recognized experts of SNL are crucial to the credibility of NAESB work products and the safety of the electronic transactions that used NAESB standards. In short, it was a tremendous benefit and we are grateful to DoE and SNL for providing such a service.

**Interaction with the NAESB cybersecurity standards for the wholesale electric market**

NAESB develops standards for wholesale and retail natural gas and electricity markets. This fact sheet has centered on the development in support of the wholesale natural gas market. That said, it is recognized that the wholesale natural gas and electricity markets are interconnected through the increased demand for natural gas by power generators.

NAESB is now focusing on the changing nature of both the natural gas and electricity markets – changes that require the two markets to more closely coordinate as natural gas increasingly becomes the fuel selected by power generators. This effort is supported by the National Petroleum Council, which also noted that the two markets were becoming increasingly interdependent. Cybersecurity and the use of electronic transactions are critical to ensuring that the markets communicate effectively not only within each market, but also across markets. Standards play a role in providing effective and efficient electronic transactions. These technical standards that support electronic transactions are built by the technical experts within the markets – with a strong understanding of the specific market requirements. As the markets interact more frequently, the policies, commercial arrangements, business practices and technical standards that support market transactions will be required to be complementary, at a minimum. Cybersecurity standards will be required to support the needs of the interdependent natural gas and electricity markets and to ensure that the commercial arrangements between both markets are protected. A review of our existing technical standards in light of these changes would be advisable.

The technical standards we have today were built in somewhat of a silo fashion. The technical standards supporting natural gas transactions were developed by the natural gas market participants. Similarly, the technical standards supporting commercial transactions for electricity were developed by the electricity market participants. Now, as these markets interact more frequently, the standards that support their transactions may be required to be consistent, at a minimum. The technical standards, of which the cybersecurity standards are a part, may be required to function interoperably for both markets – supporting the needs of the interdependent natural gas and electricity markets, to ensure that the commercial arrangements between both markets are protected.

**Conclusion**

NAESB has developed cybersecurity standards for the wholesale natural gas market that facilitate the secure transfer of transactions either via EDI or Internet web sites. Moreover, the standards are applicable to future business applications as they are identified. Lastly, the NAESB wholesale natural gas cybersecurity standards undergo continual internal and third-party review to ensure that they address evolving market needs and threats.

We hope you find this document helpful, as the subject matter is quite complex. Should you need additional information, please do not hesitate to contact the NAESB Office.

***Rae McQuade***

President, NAESB

1. <http://www.ietf.org/rfc/rfc2440.txt>, <http://www.ietf.org/rfc/rfc4880.txt> [↑](#footnote-ref-1)
2. <https://tools.ietf.org/rfc/rfc5246.txt>, , <http://tools.ietf.org/html/rfc6101> [↑](#footnote-ref-2)