NORTH AMERICAN ENERGY STANDARDS BOARD

801 Travis, Suite 1675 • Houston, Texas 77002 • **Phone:** (713) 356-0060 • **Fax:** (713) 356-0067
email: naesb@naesb.org • **Web Site Address:** www.naesb.org

April 8, 2013

Mr. Adam Sedgewick
U.S. Department of Commerce
1401 Constitution Avenue NW
Washington, DC 20230

RE: Response to the Request for Information on "Developing a Framework to Improve Critical Infrastructure Cybersecurity"

Dear Mr. Sedgewick,

Thank you for the opportunity to offer these general comments in response to the February 26, 2013 request for information from the Department of Commerce through the National Institute of Standards and Technology (NIST) concerning the development of a framework to improve critical infrastructure cybersecurity. Please find attached two documents that describe the North American Energy Standards Board (NAESB) cybersecurity related standards, their purpose, use and to which market based transactions they are intended to apply. Attachment "A" describes the standards applicable to the wholesale electricity market and attachment "B" describes the standards applicable to the wholesale natural gas market. The information contained in the documents was developed at the request of the NAESB Board of Directors and includes contributions from numerous subject matter experts in the fields of cybersecurity and energy market design.

As background, the North American Energy Standards Board (NAESB) is an American National Standards Institute (ANSI) accredited, non-profit 501(c)(6) corporation formed with the support of the Department of Energy (DoE) for the purpose of developing voluntary standards and model business practices designed to promote more competitive and efficient natural gas and electric services that streamline the transactional processes of the natural gas and electric industries. NAESB and its predecessor organization, the Gas Industry Standards Board (GISB), have developed voluntary consensus based standards in these industries for nearly twenty years with the support of the Federal Energy Regulatory Commission (FERC), the DoE, the North American Electric Reliability Corporation (NERC), the National Association of Regulatory Utility Commissioners (NARUC) and state utility commissions among other governmental and industry agencies.

NAESB maintains a membership of over three hundred corporate members that represent interests in the wholesale gas, wholesale electric, retail gas and retail electric markets. In addition, NAESB has more than two-thousand member and non-member participants active in various standards development efforts that address a wide range of subjects and levels of technical detail. While NAESB is primarily funded through its corporate memberships, the NAESB standards development process allows for all interested parties to participate and vote in the standards development activities regardless of membership status. This practice is vital to ensure that all NAESB standards have been properly vetted by the industry prior to adoption. All NAESB standards developed for the wholesale gas and wholesale electric markets are filed with the FERC and all NAESB standards developed for the retail gas and retail electric markets are submitted to NARUC and made available to all state commissions. With few exceptions, all NAESB wholesale market standards have been adopted by the FERC and mandated as federal regulation for federally jurisdictional entities through the FERC process of incorporation by reference. Many of the NAESB retail market standards have also been adopted by various state commissions and enforced in a similar manner.

Again, we are grateful for the opportunity to contribute and look forward to supporting the efforts of NIST to develop a framework to reduce the cyber risks to critical infrastructure and to supporting other federal agencies as they address Executive Order 13636.[1] We hope you find this information helpful and should you need additional information, please do not hesitate to contact the NAESB office.

With Best Regards,

Jonathan Booe

Jonathan Booe, Vice President , NAESB

Cc via email: Michael D. Desselle, Chairman of the NAESB Board of Directors
Valerie Crockett, Wholesale Gas Quadrant Vice Chair of the NAESB Board of Directors
Rae McQuade, NAESB President
William P. Boswell, NAESB General Counsel

[1] "Executive Order 13636—Improving Critical Infrastructure Cybersecurity" 78 Fed. Reg. 11739 (February 19, 2013).

NORTH AMERICAN ENERGY STANDARDS BOARD
801 Travis, Suite 1675 • Houston, Texas 77002 • **Phone:** (713) 356-0060 • **Fax:** (713) 356-0067
email: naesb@naesb.org • **Web Site Address:** www.naesb.org

NAESB WHOLESALE ELECTRIC MARKET CYBERSECURITY STANDARDS FACT SHEET

To provide additional information on the purpose and use of the NAESB cybersecurity standards related to the wholesale electric market, this fact sheet includes; a brief description of our wholesale electric market cybersecurity related standards, their purpose, to which market based transactions they were intended to apply, and their use by specific wholesale electric 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 natural gas 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 electric market

NAESB has developed wholesale electric market standards that support mutual entity authentication through the use of digital signatures, authorized certificate authorities, issuance of certificates and provision for public-private keys to access and protect market information and execute transactions -- thus supporting an infrastructure of secure electronic communications.

A trusted network of certificate authorities is one of the key ingredients needed to authenticate Internet data transfers. The NAESB business practices related to cybersecurity, in concert with the accreditation specifications for authorized certification authorities (CAs) and the program by which CAs are accredited as NAESB Authorized Certification Authorities (ACAs), provides for such a trusted network and establishes a secure public key infrastructure (PKI) for applicable NAESB wholesale electric market based transactions. This is implemented through a three pronged approach. First, the NAESB business practices related to cybersecurity describe the minimum PKI requirements of an end entity, typically a utility or independent system operator or regional transmission organization. Second, the accreditation specifications describe the minimum requirements for the CA, typically a service provider for the industry who issues the digital certificates to the end entities so that the Internet data transfers may be securely performed with the assurance of confidentiality, authentication, integrity and non-repudiation. Third, the ACA process describes the procedures by which a CA may become a NAESB ACA and issue digital certificates to the end entities. The end entities are responsible for creating their own public-private key pairs. The ACA issues digital certificates using the public key of an end entity.

So, how does the mutual entity authentication work as described in the standards, the accreditation process and the minimum requirements of the certificate authorities? As best described in “Entity Authentication Using Public Key Cryptography (FIPS PUB 196),” entities in two computers authenticate their identities to one another by two challenge-response protocols. In this case, it is the end entity and the service provider operating the system – such as OASIS or the Registry participating in the mutual entity authentication. The FIPS publication goes on to note that “These protocols may be used during session initiation, and at any

NAESB WHOLESALE ELECTRIC MARKET CYBERSECURITY STANDARDS FACT SHEET

other time that entity authentication is necessary. The challenge-response protocols are derived from an international standard for entity authentication based on public key cryptography, which uses digital signatures and random number challenges. Authentication based on public key cryptography has an advantage over many other authentication schemes because no secret information has to be shared by the entities involved in the exchange. A user attempting to authenticate oneself must use a private key to digitally sign a random number challenge issued by the verifying entity. This random number is a time variant parameter which is unique to the authentication exchange. If the verifier can successfully verify the signed response using the user's public key, then the user has been successfully authenticated."

The standards language specific to this description on public key cryptography use notes that the end entities acknowledge as the industry's endorsement of public key cryptography (using asymmetric algorithms such as RSA) which utilize public key certificates to bind a person's or computer system's public key to its entity, and to support symmetric encryption (using symmetric algorithms such as AES) – which means that the same key is used to encrypt and decrypt a message. Therefore, the standards support a hybrid system that uses both symmetric and asymmetric algorithms to provide the needed protection, yet also allow for manageable keys and encryption/decryption transaction speed.[1]

The Accreditation Requirements for ACAs includes specifications for certificate uses, assurance levels, identification and authentication, certificate lifecycles, facility management and operations controls, identification of auditable events, maintenance of audit logs, technical security controls, key sizes, activation data, lifecycle security controls, security management controls, network security controls, certificate profiles and CRL profiles.

Application of the NAESB cybersecurity standards in the wholesale electric market

NAESB's long-standing support for open standards has served to create 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 and specifications is intended to facilitate the availability of interoperable PKI products from multiple vendors.

The NAESB cybersecurity related standards and specifications facilitate an infrastructure to secure electronic communications, and they establish the obligations of both ACAs and end entities, but the standards do not specify how certificates issued by ACAs may be used in specific software applications or electronic transactions within the guidance of NAESB. Our business practice standards do not apply to nor impact the reliability of the bulk power grid – that is the domain of the North American Electric Reliability Corporation (NERC). The cybersecurity related standards and specifications were developed to apply to business practices and processes for electricity reservations and scheduling. For use, the standards apply to the Electric Industry Registry, e-Tagging and OASIS systems, and to other electronic transactions deemed

[1] http://support.microsoft.com/kb/257591

NAESB WHOLESALE ELECTRIC MARKET CYBERSECURITY STANDARDS FACT SHEET

mutually agreeable by the transacting parties. The entities using the standards and program are the utilities, ISOs, RTOs, third party service providers issuing certificates as NAESB ACAs, entities providing information to the Electric Industry Registry or accessing information from the Electric Industry Registry, and entities requiring e-Tags. The Electric Industry Registry is a central repository for commercial industry information defining the roles played by entities to support the electronic transactions related to reservations and scheduling of wholesale power. E-Tags are used to identify interchange transaction information between parties resulting in the physical flow of electricity from one point to another in the wholesale electric market.

For specifics on the cybersecurity standards, the standards require the use of a PKI using X.509 v3 digital certificates, issued by NAESB ACAs, to provide for (1) confidentiality: the assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended, (2) authentication: the assurance to one entity that another entity is who he/she/it claims to be, (3) integrity: the assurance to an entity 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: a party cannot deny having engaged in the transaction or having sent the electronic message.

While the cybersecurity related standards and specifications could be applied more broadly, they were defined for these purposes. As other electronic transactions in the wholesale electric market are determined to require such entity authentication, they too could be included as applicable.

Regulatory Implications of the NAESB cybersecurity standards

The cybersecurity standards and the accreditation requirements were developed to align with industry best practices for PKI as prescribed by the National Institute of Standards and Technology (NIST) in publication NIST Special Publication (SP) 800-57 Part 1, 800-130 and 800-131A, Internet Engineering Task Force PKI guidelines and standards (including but not limited to RFC 3280, 3647, and 4210). The cybersecurity standards have been provided to the Federal Energy Regulatory Commission (FERC) as part of Docket No. RM05-5-022, on January 29, 2013, and an update report regarding the development and revisions of these cybersecurity standards were provided to FERC on November 30, 2012. If FERC determines to adopt the standards, then they would become mandatory for jurisdictional entities – typically the utilities and independent system operators and regional transmission owners who are reflected in the standards as end entities. Should the standards become mandatory through actions of FERC, the administration that accompanies compliance with the standards would be a function of FERC.

NAESB Data Privacy Standards in Support of Smart Grid

The NAESB data privacy standards were developed to support the retail electric market as it implements smart grid applications. These standards do not apply to the wholesale electric market; however, provide a better understanding of the work undertaken to support cybersecurity needs, so we have included this section. The data privacy standards define the responsibilities of utilities and third party service providers as they exchange and maintain smart meter customer energy usage data. The Smart Grid Interoperability Panel has requested changes that are now under consideration, including:

- additional cybersecurity requirements for supporting privacy as well as traditional cybersecurity requirements for third party access to smart meter-based information,
- utility privacy requirements that utilities should undertake for the privacy of retail customer data, including a requirement that contracted agents protect the data throughout the entire data lifecycle,
- utility provision of information to customer s to support customer protection of data after the data has been transferred to a third party, and
- third party identity verification standards in support of smart-meter based information.

Future Developments for the NAESB cybersecurity standards

There are several items that are identified for cybersecurity standards development in 2013, and as our organization receives requests throughout the year, more activity could be identified. On our 2013 annual plan for standard development, the following items have been approved for development:

- review and develop standards as needed to support adequate session encryption (SSL/TLS issues: US-Cert Vulnerability Note VU#864643),
- review the FERC Report, "Report on Use of North American Energy Standards Board Public Key Infrastructure Standards," Docket No. EL12-86-000, issued on August 27, 2012, to determine which standards changes are needed to be responsive to suggestions made by the Commission, and
- review annually at a minimum, the accreditation requirements for ACAs to determine if any changes are needed to meet market conditions.

Also, there have been initial dialogs held with the U.S. Department of Energy (DoE) regarding a surety assessment for the technical standards of NAESB, which would include the cybersecurity standards. Should this surety assessment take place, it would be the third assessment conducted by Sandia National Laboratories (SNL) on behalf of DoE. The form of the surety assessments looked much like a series of audit findings, 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. NAESB's responses also took a form much like a response to an audit. For each finding and recommendation, a response was prepared that identified the action to be taken and when it would be completed. These independent surety assessments by the recognized experts of SNL were crucial to the credibility of our 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 natural gas 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 electric 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 becomes more and more the fuel selected by power generators. This effort is supported by the National Petroleum Council, who 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 usage plays 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 market requirements. As the markets interact more frequently, the policy, commercial arrangements, business practices and technical standards will be asked to reflect those interactions, rather than present barriers. 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 as an umbrella over 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

The cybersecurity standards (referenced by NAESB as WEQ-012) were developed to apply to business practice standards and processes for wholesale electricity reservations and scheduling or any future business applications identified as applicable with mutual agreement by the transacting parties. They have been recently revised to ensure that they address market needs and the revisions were provided to FERC for its consideration.

NAESB WHOLESALE ELECTRIC MARKET CYBERSECURITY STANDARDS FACT SHEET

The announcement of the effort to modify the WEQ-012 standards and put the credentialing process in place was posted for public access and the status reported at many NAESB Board and Executive Committee meetings, open to all interested parties. The recommendations for the revisions were adopted by the subcommittee with no negative votes cast and received overwhelming approval by the Executive Committee and members during the ratification process.

NORTH AMERICAN ENERGY STANDARDS BOARD
801 Travis, Suite 1675 • Houston, Texas 77002 • **Phone:** (713) 356-0060 • **Fax:** (713) 356-0067
email: naesb@naesb.org • **Web Site Address:** www.naesb.org

Attachment B
April 8, 2013
Page 1 of 4

NAESB WHOLESALE 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] used for PGP, notably, IETF RFC 4880, and the cybersecurity industry is moving towards use of TLS[2] rather than SSL,

[1] http://www.ietf.org/rfc/rfc2440.txt, http://www.ietf.org/rfc/rfc4880.txt
[2] https://tools.ietf.org/rfc/rfc5246.txt, , http://tools.ietf.org/html/rfc6101

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, who 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

NAESB WHOLESALE GAS MARKET CYBERSECURITY STANDARDS FACT SHEET

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.