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

November 30, 2012
Filed Electronically

The Honorable Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street N.E., Room 1A
Washington, D.C. 20585

RE: NAESB Progress Report on the Public Key Infrastructure Standards (WEQ-012) and Public Key
        Infrastructure Related Standards Development

Dear Ms. Bose:

The North American Energy Standards Board ("NAESB") herewith submits this status report to the Federal Energy
Regulatory Commission ("FERC" or "Commission") describing the NAESB standards development efforts related
to Public Key Infrastructure ("PKI"). This standards development effort has resulted in modifications to the
NAESB WEQ-012 PKI standards, the development of the NAESB Accreditation Requirements for Certification
Authorities Specification and the NAESB Authorized Certificate Authority Process. In addition, NAESB has
adopted conforming changes to NAESB WEQ-000 Abbreviations, Acronyms, and Definition of Terms, the NAESB
WEQ-002 Open Access Same-Time Information Systems Standards and Communication Protocols standards, and is
in the process of adopting modifications to the NAESB WEQ-004 Coordinate Interchange standards. It is expected
that the conforming changes to WEQ-004 will be adopted and ratified by NAESB before the end of the year.[1]

The purpose of this status report is to inform the Commission of the actions taken by NAESB related to the PKI
standards development effort to date and to prepare the Commission for an anticipated supplemental filing to the
NAESB Wholesale Electric Quadrant Version 003 standards report, which will include the updated WEQ-000,
WEQ-002, WEQ-004 and WEQ-012 standards.

The report is being filed electronically in Adobe Acrobat® Portable Document Format (.pdf). The report is also
available on the NAESB web site (www.naesb.org). Please feel free to call me at (713) 356-0060 or refer to the
NAESB website (www.naesb.org) should you have any questions or need additional information regarding NAESB
work products.

Respectfully submitted,

Rae McQuade

Ms. Rae McQuade
President & COO, North American Energy Standards Board

---

[1] The NAESB standards and specifications referenced in this report are reasonably available to the public through multiple methods. To access
the standards or specifications at no cost, NAESB will provide a limited copyright waiver for evaluation purposes using a product called Locked
Lizard (http://www.locklizard.com). To request a waiver, please contact the NAESB office or follow the instructions in the following document:
http://www.naesb.org/pdf/ordrform.pdf.

November 30, 2012

cc: Chairman Jon Wellinghoff, Federal Energy Regulatory Commission
Commissioner, Tony Clark, Federal Energy Regulatory Commission
Commissioner, Cheryl LaFleur, Federal Energy Regulatory Commission
Commissioner Philip D. Moeller, Federal Energy Regulatory Commission
Commissioner John Norris, Federal Energy Regulatory Commission

Mr. Joseph McClelland, Director Office of Energy Infrastructure Security, Federal Energy Regulatory Commission
Mr. Michael Bardee, Director Office of Electric Reliability, Federal Energy Regulatory Commission
Mr. David Morenoff, Acting General Counsel, Federal Energy Regulatory Commission

Mr. Mason Emnett, Associate Director, Office of Energy Policy and Innovation, Federal Energy Regulatory Commission
Mr. Michael Goldenberg, Senior Attorney, Office of General Counsel, Federal Energy Regulatory Commission
Ms. Jamie L. Simler, Director, Office of Energy Policy and Innovation, Federal Energy Regulatory Commission

Mr. Michael Desselle, Chairman and CEO, North American Energy Standards Board
Mr. William P. Boswell, General Counsel, North American Energy Standards Board

Mr. Charles Berardesco, General Counsel, North American Electric Reliability Corporation
Mr. Mark Lauby, Vice President and Director, Standards, North American Electric Reliability Corporation

November 30, 2012

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Standards for Business Practices and	)	**Docket No. RM 05-5-000**
Communication Protocols for Public Utilities	)	**Docket No. RM 05-5-022**

STATUS REPORT OF THE NORTH AMERICAN ENERGY STANDARDS BOARD

The North American Energy Standards Board ("NAESB") is voluntarily submitting this status report to the Federal Energy Regulatory Commission ("FERC" or the "Commission") in the above referenced docket to inform the Commission of the NAESB Public Key Infrastructure ("PKI") standards development efforts to date.

On September 18, 2012, NAESB filed the NAESB Wholesale Electric Quadrant ("WEQ") Version 003 standards report[2] with the Commission in Docket Nos. RM 05-5-000, RM 05-17-000, and RM 07-1-000. At that time, a recommendation proposing modifications to the WEQ-012 PKI standards had been approved by the WEQ Executive Committee ("EC") but had not been ratified by the NAESB membership, and the NAESB Open Access Same-time Information Systems ("OASIS") Subcommittee and the Joint Electric Scheduling ("JESS") Subcommittee were in the development phases of recommendations addressing conforming changes to the OASIS standards (WEQ-001, WEQ-002, WEQ-003 and WEQ-013) and coordinate interchange standards (WEQ-004) to support the proposed WEQ-012 modifications. As such, NAESB is supplementing the September 18, 2012 WEQ Version 003 report to the Commission with this status update and intends to submit a subsequent report including the revised WEQ-000, WEQ-002, WEQ-004 and WEQ-012 standards at the beginning of 2013 upon ratification of the final PKI related standard by the membership. The purpose of this status report is to inform the Commission of the actions taken by NAESB related to the PKI standards development effort to date and to give notice of the supplemental report expected to be submitted to the Commission after the first of the year.

---

[2] NAESB Version 003 Standards, Docket No. RM05-5 et al, *available at*: http://www.naesb.org/pdf4/ferc_091812_weq_version003_report.pdf (submitted September 18, 2012).

![NAESB logo]

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

November 30, 2012

Background Information

      The existing WEQ-012 standards developed in 2006 and adopted by the Commission in 2008,[3] were drafted to provide cybersecurity standards for use in commercial transactions – namely OASIS based transactions, and to support the transition of the North American Electric Reliability Corporation ("NERC") Transmission System Information Network ("TSIN") registry from NERC to NAESB. The registry is a tool that serves as a central repository of information required for commercial transactions involving the scheduling of power through electronic tagging in the e-Tag system. Through discussions between NERC and NAESB leadership, it was determined that the registry would be more appropriately maintained by NAESB given the tool's commercial function. After an extended period of planning, NERC and NAESB, through the JESS subcommittee, drafted a functional specification for the development of the Electric Industry Registry ("EIR"), which would serve as the tool to replace the NERC TSIN, and issued a request for proposal[4] for an EIR registry administrator to facilitate the transition. After evaluating the proposal, the NAESB Managing Committee and NERC leadership selected Open Access Technology International, Inc. ("OATI") to serve as the registry administrator in the summer of 2010.

      A requirement of the functional specification for the EIR was that it employ a PKI security scheme, which necessitates the use of digital certificates issued by certification authorities. To facilitate the transfer, NAESB leadership recognized that action would need to be taken to develop a program to approve certificate authorities as NAESB Authorized Certificate Authorities ("ACA") and to modify the WEQ-012 PKI standards to reflect updates to technology and current market conditions related to the secure transfer of information. To accomplish this, the NAESB Board Certification Program Committee was reactivated in April 2011 to develop a program for the authorization of certificate authorities and the WEQ EC created the PKI Subcommittee in August 2011 to review and revise the WEQ-012 standards. These activities have led to the creation of the Board of Directors approved NAESB Authorized Certificate Authority Process, the NAESB Accreditation Requirements for Certificate Authorities Specification ("Accreditation Specification") created by the PKI Subcommittee, modifications to the NAESB WEQ-000, WEQ-002, WEQ-004 and WEQ-012 standards and the NAESB WEQ Electronic Tagging

---

[3] The FERC adopted NAESB standards in FERC Order No. 676-C on July 21, 2008 and the order can be access from the FERC web site or through this link: http://elibrary.ferc.gov/idmws/file_list.asp?accession_num=20080721-3055.
[4] The request for proposal is available at: http://www.naesb.org/pdf4/tsin_registry_rfp_022210.pdf

November 30, 2012

Functional Specification. All of these efforts have been orchestrated to coincide with the registry transition which took place on November 13, 2012. [5]

Upon ratification of the modifications to the WEQ-004 standards at the end of December, NAESB will submit a report to the Commission noting their completion and a description of the WEQ-000, WEQ-003, WEQ-004 and WEQ-012 standards modifications.

NAESB Authorized Certificate Authority Process

On April 4, 2011 the Board Certification Program Committee met for the first time since 2007 to evaluate the WEQ-012 standards and initiate the development of a process to support the authorization of certificate authorities. Over the course of five months, the committee met a total of six times through August 2011 to develop a process by which certificate authorities may seek approval by NAESB as an ACA. The process requires the submission of several documents, which initially included an attestation of compliance with the NAESB WEQ-012 PKI business practice standards, proof of compliance through an audit letter and documentation indicating whether the applying certificate authority has undergone an SSAE 16 SOC3 or WebTrust audit. The process also defined the terms surrounding revocation and notification requirements. On August 29, 2011, the Committee unanimously adopted the draft Authorized Certificate Authority Process with the understanding that there may be the need for revisions upon completion of the update to the WEQ-012 PKI standards. The Authorized Certificate Authority Process was presented to the Board of Directors during the September 22, 2011 meeting and approved without opposition, noting the caveat that modifications may be required upon completion of the revisions to the WEQ-012 standards.

On September 14, 2012[6], after WEQ EC approval of the modifications to the WEQ-012 standards and the Accreditation Specification, the Board Certification Program Committee reconvened to review the Authorized Certificate Authority Process in light of the EC action. During this meeting the committee agreed to modify the board approved process to include compliance with the newly created Accreditation Specification in addition to other updates identified by the PKI Subcommittee during the standards development process. The updated and

---

[5] Distribution related to the registry transition is available at: http://www.naesb.org/pdf4/eir_distribution_101812.pdf

[6] The minutes from this meeting are available at: http://www.naesb.org/pdf4/cpc091412mn.doc

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

November 30, 2012

current version of the Authorized Certificate Authority Process was adopted by the Board of Directors on September 20, 2012.[7]

<u>NAESB WEQ-012 PKI Standards Modifications and Accreditation Specification</u>

In August of 2011, the NAESB WEQ EC created the PKI Subcommittee for the purpose of reviewing and revising the WEQ-012 standards to reflect updates to technology and current market conditions related to the secure transfer of information. As with the Authorized Certificate Authority Process effort, this action was taken at the direction of NAESB leadership to coincide with the transfer of the NERC TSIN and the implementation of the EIR. The PKI Subcommittee was chaired by technology company 8760, Inc. and the subcommittee held its first meeting on September 22, 2011. Over the course of ten months, through July 2012, the subcommittee met a total of fourteen times to develop the recommended revisions to the WEQ-012 standard and the accreditation specification. Through subcommittee discussion, it was determined that it would be appropriate to split the previous version of the WEQ-012 standard into two documents; one document, the revised WEQ-012 standard, defining the standards that should apply to end entities implementing PKI transactions, and a second document, the Accreditation Specification, containing the requirements that should be met by certificate authorities seeking approval as a NAESB ACA. This action was taken in recognition that certificate authorities are not necessarily subject to the Commission's jurisdictional authority granted through the Federal Power Act and because a requirements specification, rather than a NAESB standard, may be modified through an expedited NAESB process in the event that technology advances are needed in response to a security threat. As such, the requirements pertaining to certificate authorities were extrapolated from the existing WEQ-012 standard and included in the Accreditation Specification. After the division both documents were reviewed and modified to reflect technology and security updates that are necessary for a secure PKI implementation.

With very few exceptions, the details of theWEQ-012 standard and Accreditation Specification were drafted with unanimous support of the subcommittee. A single issue concerning the required validity period of ACA root certificates required a vote and resulted in a compromised position that was adopted with a single vote in opposition. A few participants supported limiting the life of the ACA root certificates to 20 years, while a majority of participants recommended 20 years with the opportunity for an extension to 30 years if certain requirements were

---

[7] The minutes from this meeting are available at: http://www.naesb.org/pdf4/bd092012dm.docx

November 30, 2012

met. The participants supporting the longer limit advocated that a 30 year life cycle is the current industry standard and that setting a lower limit would be overly burdensome and costly to the industry, as existing certificates would have to be reissued and modifications to certificate authorities' processes would be required. Participants supporting a shorter life cycle argued that a shorter time period would significantly reduce the risk of a security breach, as the root certificates would be vulnerable for a reduced amount of time. As a compromise the subcommittee set a maximum life of 20 years for all certificate root keys, unless the certificate qualified to be grandfathered under the condition that there have been no security breaches to certificate authority operations within 10 years and that all key sizes in the certificate chain are at least 2048 bit. The compromise resolution for key lifetimes is based on guidelines contained in section 6.3.2 of the X.509 Certificate Policy for the Federal Bridge Certification Authority and is consistent with the National Institute of Standards and Technology ("NIST") recommended key lifetimes contained in NIST SP 800-57, section 5.6.2. As previously noted the compromise was approved during the June 14, 2012 meeting and supported by all but one participant.

The Accreditation Specification as a whole was also voted out of the subcommittee on June 14, 2012 with no votes in opposition. It was distributed for a thirty day public comment period on June 25, 2012.   The subcommittee next met on July 3, 2012 and July 9, 2012 to review of the remaining WEQ-012 standards, make modifications and vote on a recommendation. The WEQ-012 PKI standards modifications were distributed for a thirty day public comment period on July 10, 2012. On August 15, 2012 and August 16, 2012, the subcommittee met to review and develop a set of late comments in response to the four sets of comments submitted on the Accreditation Specification and the six sets of comments submitted on the WEQ-012 standard. All comments, including the late comments submitted by the subcommittee, were presented to the WEQ EC during the August 21, 2012 meeting.[8] Both recommendations were approved as recommended in the late comments of the PKI Subcommittee and modified during the meeting with only one vote in opposition. The modifications to the WEQ-012 standards were submitted for membership ratification and ratified on October 4, 2012. As the Accreditation Specification is, in fact, a specification rather than a standard, the specification did not require membership ratification and will not be included in the supplemental filing made by NAESB for Version 003.

Modifications to NAESB WEQ-000, WEQ-002, and WEQ-004

---

[8] The minutes from this meeting are available at: http://www.naesb.org/pdf4/weq_ec082112fm.docx

NAESB

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

November 30, 2012

During the review of the comments submitted on the proposed modifications to the WEQ-012 standards and the Accreditation Specification, the PKI Subcommittee recognized that the applicability of the standard to specific business transactions had not been defined in the standard. The subcommittee determined that the WEQ-012 standard should be applicable to transactions on OASIS and through the e-Tag system as defined in the WEQ-001, WEQ-002, WEQ-003, WEQ-004 and WEQ-013 standards. As such, specific language was proposed to section 1.3.4 of the WEQ-012 standard in the late comments of the subcommittee provided for WEQ EC consideration. During the review and adoption of the standards modifications, including the proposed language changes related to applicability, the WEQ EC recommended that the OASIS and JESS subcommittees review the OASIS and Coordinate Interchange standards to determine what modifications would be required to enable the WEQ-012 standard to provide a standard method for secured access to OASIS and e-Tag applications. The WEQ EC also asked the OASIS and JESS subcommittees to expedite the development of the complimentary standards as part of the NAESB full-staffing process.

The WEQ OASIS Subcommittee met twice, for a total of six hours, with members of the WEQ PKI Subcommittee to develop a recommendation proposing modifications to the WEQ-000 and WEQ-002 standards. The recommended modifications to the WEQ-002 Standards and Communication Protocols require that transmission service information providers verify certain information in the EIR before establishing a valid user account on OASIS, specifically that the subscriber certificate is issued by a NAESB ACA. In addition, technical standards to support the implementation of the WEQ-012 standards in the OASIS system and the transition of the registry from NERC to NAESB were made to the WEQ-002 standards. Two acronyms from the WEQ-012 standard were proposed for inclusion in WEQ-000 Abbreviations, Acronyms and Definitions of Terms. The subcommittee voted out the recommendation on September 7, 2012 and after a thirty day comment period, the recommendation was presented to the WEQ EC during the October 23, 2012 meeting.[9] During that meeting, the WEQ EC reviewed the comments submitted on the recommendation and made a modification in response to a request from the New York ISO to require the check of the assurance level contained in the certificate at the time of registration rather than each time a party connects to OASIS. The recommendation, as revised, passed a super majority vote without opposition was distributed for a membership ratification period that concluded on November 28, 2012.

---

[9] The minutes from this meeting are available at: http://www.naesb.org/weq/weq_ec.asp

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

November 30, 2012

The WEQ JESS initiated efforts to develop complimentary WEQ-004 standards and consistent modifications to the WEQ Electronic Tagging Functional Specification Version 1.8.1 on September 6, 2012. Over the course of three meetings the JESS developed two recommendations, one which contained proposed modifications to the WEQ-004 standards[10] and one that proposed consistency revisions to the e-Tag Specification Version 1.8.1[11] to support the WEQ-012 standards and the EIR transition. The recommendation related to the Coordinate Interchange standards proposed the addition of a single standard requiring all e-Tag communications be secured using digital certificates issued by a NAESB ACA in accordance with the WEQ-012 standards.

The thirty-day industry comment period for both recommendations concluded on November 5, 2012 and the JESS met on November 7, 2012 to review the single set of comments submitted by the NAESB Standards Review Subcommittee providing an internal consistency suggestion. At the request of the chair of the WEQ EC, a notational ballot was distributed on November 13, 2012 to the WEQ EC requesting their vote on the two recommendations. The notational ballot period concluded on November 27, 2012 and both recommendations, as modified in the late comments submitted by the JESS, received the required votes in support for approval. The WEQ-004 standard[12] was distributed for a thirty-day membership ratification period which ends on December 28, 2012. Like the Accreditation Specification, the modified e-Tag Specification Version 1.8.1 is not considered a NAESB standard and will not be subject to membership ratification or included in the NAESB supplemental filing for Version 003.

Next Steps

All certificate authorities that have expressed interest in becoming a NAESB ACA are currently in a pending status and have not been officially credentialed by NAESB. NAESB has not requested that the ACAs pending approval submit documentation in compliance with the Authorized Certificate Authority Process and will not do so until two activities have been finalized. First, the WEQ-012 standard and complementary modifications to WEQ-000, WEQ-002 and WEQ-004 standards are complete and filed with the Commission. As previously noted this will take place after the first of the year. Second, globally unique object identifiers must be obtained by NAESB

---

[10] The recommendation is available at: http://www.naesb.org/member_login_check.asp?doc=weq_2012_api4b_part1_rec.doc
[11] The recommendation is available at: http://www.naesb.org/pdf4/weq_2012_api4b_part2_rec.doc
[12] The recommendation as approved by the WEQ EC is available at:
http://www.naesb.org/member_login_check.asp?doc=weq_100512_weq_jess_part1_late.doc

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

November 30, 2012

and incorporated into the Accreditation Specification. As a requirement of the Accreditation Specification, certificates issued by an ACA must include a certificate policy extension that asserts compliance with an assurance level specified in the accreditation specification. For an ACA to comply, a globally unique object identifier should be assigned to each of the assurance levels and made part of an ACA certificate. NAESB is currently in the process of obtaining the globally unique object identifiers through the American National Standards Institute ("ANSI"). Once delivered by ANSI, NAESB will incorporate the object identifiers into the Accreditation Specification and give notice to the ACAs pending approval. Currently, there are four ACAs pending approval and all have been heavily involved in the NAESB PKI standards development effort or have followed its progress. As subject matter experts, their participation is crucial and their contributions have been instrumental in shaping the requirements for both ACAs and the end entities that will employ PKI security.

Finally, the WEQ EC has made a recommendation that an item be added to the 2013 WEQ Annual Plan to ensure that issues raised in the Commission's "Report on the Use of North American Energy Standards Board Public Key Infrastructure Standards" on August 27, 2012 in Docket No. EL 12-86-000 are addressed.[13] As recommended by the Commission, the NAESB PKI Subcommittee will review the root key validity period issue and discuss a possible modification at the beginning of 2013. As always, NAESB appreciates the opportunity to provide this status report and to support the directives of the Commission.

---

[13] The report is available at: http://www.ferc.gov/EventCalendar/Files/20120827175825-EL12-86-000.pdf