**NAESB Authorized Certification Authority Process**

December 8, 2016

Schematic:

Subscriber – User of the NAESB WEQ-012 Standards

Authorized Certification Authority (ACA)

Independent Third Party Auditor

NAESB

The subscriber employs an Authorized CA as noted in the WEQ-012 standards

NAESB requires an affidavit certifying material compliance with the WEQ-012 specification signed under oath by a senior executive officer of the Authorized Certification Authority.

The third party auditor is independent of the Subscriber and the Authorized Certification Authority and is employed by the ACA to review the ACA’s compliance with the NAESB requirements.

The following are the components of the process to be used by NAESB to certify, and maintain the certification of Authorized Certification Authorities (ACAs):

1. ACA Certification

The NAESB Certification Program utilizes a self-certification format. To be initially certified, the candidate certificate authority seeking ACA Certification (“Candidate”) must submit to NAESB:

* 1. An affidavit, signed by an Officer or Principal, that the Candidate meets the WEQ-012 requirements as specified in Section 5 for the applicable assurance level(s) and version(s) and certifies that its answers are accurate and truthful. The affidavit is modeled on similar statements made under Sarbanes-Oxley.
	2. The attestation pursuant to Section 2a(i) and the indication as noted in Section 2(a)(ii).

NAESB does not warrant or guarantee that the ACA’s services comply with the WEQ-012 standard, perform as intended, or comply with representations made by the ACA.

The ACA is not required to be a member of NAESB, but must possess a current and legal copy of relevant NAESB standards.

An ACA may display the applicable valid NAESB Certification Mark for applicable version(s) and assurance level(s) provided by NAESB on its web site or documentation for as long as the ACA remains NAESB certified.

After the candidate completes the self-certification steps in Section 1.a and 1.b above and achieves NAESB certification, NAESB will report to the North American Electric Reliability Corporation (NERC) the name of the candidate and that the candidate is and ACA. The certificate authority will immediately be authorized to display the NAESB certification mark and will be authorized to claim compliance with the NAESB Accreditation Requirements for Authorized Certification Authorities. NAESB will provide notice to the industry regarding the certification of a new ACA and/or renewal of an existing ACA. This notice will be provided through the notice functionality with the NAESB Electric Industry Registry (EIR) and distributed one (1) business day prior to the date entities must accept certificates issued by the ACA.

NAESB will maintain contact information for all ACAs on its web site.

2. Auditing/Renewal

1. To maintain NAESB Certification, the ACA must submit annually to NAESB:

i. an attestation, such as an audit management letter by a Qualified Auditor, that the ACA is compliant in all material respects with the WEQ-012 standards as specified in Section 5 for the applicable assurance level(s) and version(s).

ii. an indication of whether the ACA has received any of the following:

(a) an unqualified audit from the most recent SSAE 16 SOC 3 engagement employing the version of the AICPA Trust Services Principles, Criteria and Illustrations approved for use by the AICPA for the applicable audit period, including the date completed

(b) an unqualified audit from the most recent WebTrust engagement, employing the version of the AICPA Trust Services Principles, Criteria and Illustrations approved for use by the AICPA for the applicable audit period, which report indicates the ACA has permission to post the **AICPA/CICA *WebTrust Seal*** of assurance on the ACA’s website, including the date completed.

1. The attestation in 2(a)(i) must be performed by an independent, unaffiliated 3rd party auditor (“Qualified Auditor”) that is experienced with SSAE 16 SOC 3 or WebTrust engagements employing the AICPA Trust Services Principles, Criteria and Illustrations.
2. The above information will be provided to NAESB contemporaneously with the ACA’s making the report available to other organizations.
3. The ACA may incorporate the NAESB Accreditation Requirements for Authorized Certification Authorities and WEQ-012 requirements into the audit processes it utilizes to perform related audits of its ongoing business.
4. No auditing of the ACA’s subscribers is necessary.
5. An ACA must be recertified by NAESB if there is a purchase, sale or merger of the Authorized Certification Authority by/with another entity.

3. Revocation

a. NAESB may rescind an ACA’s Certification for cause at any time by providing 30 days’ notice in writing to the ACA. ACAs that receive a rescission notice from NAESB are required to notify all affected certificate holders within 5 days that their NAESB Certification has been rescinded and their Certificates will no longer be valid.

b. NAESB may revoke the certification of an ACA if:

* + 1. The ACA fails to submit to NAESB, in a timely manner, the submissions of Section 2(a).
		2. The submissions of Section 2(a) indicate that the ACA is no longer in compliance with the WEQ-012 requirements as specified in Section 5.

4. ACA Notification Requirements

a. The ACA shall notify NAESB and its affected subscribers, as specified by the applicable jurisdictional agency’s notification requirements (for example, NERC EOP-004[[1]](#footnote-1)), upon becoming aware of an applicable security breach. If there are no notification requirements from an applicable jurisdictional entity, the notification should take place by the close of the next business day. An applicable breach shall include breaches that compromise the integrity/trustworthiness of the “root certificate” and/or the certificate signing policies that are used to produce digital certificates.

b. The ACA shall notify NAESB and its subscribers a minimum of 90 days in advance of any plans to cease performing the Certification Authority function or intent to withdraw from NAESB’s list of ACAs. NAESB will provide notice to the industry of withdrawal of an ACA through the notice functionality within the NAESB EIR after notification by the ACA.

c. The ACA shall, within one (1) business day, notify NAESB if any End Entity seeking a digital certificate is not incorporated in or does not own assets in or does not conduct business in the United States, Canada, or Mexico.

5. Compliance with WEQ-012 Requirements

a. In complying with the WEQ-012 requirements when issuing certificates for WEQ-012 applications, ACAs must comply with:

- the provisions of the NAESB WEQ-012 Public Key Infrastructure Business Practice Standards and Models,

- the NAESB WEQ-022 Electric Industry Registry Business Practice Standards,

- the NAESB Accreditation Requirements for Authorized Certification Authorities, and

- this NAESB Certification Program to be considered an ACA.

b. All WEQ-012 applications (e.g., OASIS) secured under these Business Practice Standards WEQ-012 must permit access to any legitimate user that presents a valid electronic Certificate issued by an Authorized Certification Authority at the minimum required assurance level, or higher, as specified for the applicable application.

c. In complying with the WEQ-012 requirements, when issuing certificates for use within the energy industry for other than WEQ-012 applications, ACAs must comply with:

- the provisions of the NAESB WEQ-012 Public Key Infrastructure Business Practice Standards and Models, except provisions in WEQ-012-1.9.1, WEQ-012-1.3.3, and WEQ-012-1.4.3, which require End Entity registration within the NAESB EIR,

- the NAESB Accreditation Requirements for Authorized Certification Authorities, and

- this NAESB Certification Program to be considered an ACA.

1. NERC Emergency Preparedness and Operations EOP-004-1 Disturbance Reporting, <http://www.nerc.com/files/EOP-004-1.pdf> , includes requirements for submitting notifications of disturbances. [↑](#footnote-ref-1)