##### November 27, 2017

**TO:** All Interested Parties

**FROM:** Elizabeth Mallett, NAESB Deputy Director

**RE: Update to the Board of Directors – WEQ Cybersecurity Subcommittee (CSS)**

In February, the Wholesale Electric Quadrant (WEQ) Executive Committee will consider a recommendation from the WEQ Cybersecurity Subcommittee (CSS) concerning 2017 WEQ Annual Plan Item 4.a, which tasked the subcommittee with a review of the Public Key Infrastructure (PKI) Business Practice Standards and the accreditation requirements for Authorized Certification Authorities (ACAs) to determine if any changes are needed to meet market conditions. When the WEQ CSS first discussed this topic in July, the participants reviewed the new version of the National Institute of Standards and Technology (NIST) Special Publication, *Digital Identity Guidelines,*[[1]](#footnote-1) released in June of 2017. As the NAESB Accreditation Requirements for ACAs contains a section on identity proofing that references an earlier version of those NIST guidelines, the subcommittee considered any possible revisions to be made to the Accreditation Requirements for ACAs. On October 12, 2017, the WEQ CSS voted out the recommendation which proposed revisions modifying Section 2.2.2 Authentication of Subscribers of the NAESB Accreditation Requirements for Authorized Certification Authorities to provide new mappings for the identity proofing process methods. Additionally, a requirement related to an action that NAESB may take was deleted from Section 3.7.1 as the concept is adequately addressed by the Authorized Certification Authority Process. Furthermore, the recommendation also corrects the usage of the terms “Subscriber”, “Applicant”, and “End Entity”. No comments were submitted on the recommendation during the thirty-day industry comment period that concluded on November 10, 2017.

Adopted by the WEQ Executive Committee on October 24, 2017, the second WEQ CSS recommendation developed this year determined that no action was needed in response to 2017 WEQ Annual Plan Item 4.b. This annual plan item required the WEQ CSS to evaluate and modify standards as needed to support and/or complement the current version of the NERC Critical Infrastructure Protection (CIP) Standardsand any other activities of NERC and the FERC related to cybersecurity. As part of these discussions, the subcommittee reviewed the May 11, 2017 Executive Order, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*[[2]](#footnote-2) and determined that there was no impact on the NAESB WEQ Business Practice Standards. Additionally, the subcommittee reviewed NERC Project 2016-02 Modifications to CIP Standards and NERC Project 2016-03 Cyber Security Supply Chain Risk Management and found no modifications to the standards to be necessary.

In response to the directives from the July 21, 2016 FERC Order No. 829[[3]](#footnote-3), NERC, in Project 2016-03, addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with the Bulk Electric System (BES) operations. As any of the developments on this project could have potentially modified the CIP standards, the WEQ CSS monitored the efforts. NAESB staff coordinated with NERC staff on NERC Project 2016-03 to determine whether the NERC Reliability Standards being developed as part of the effort would impact tools referenced by NAESB standards, such as OASIS and the EIR, or if the NAESB ACAs that issue digital certificates would be considered vendors under the new NERC standards. After receiving a statement from NERC that the CIP Reliability Standards would only be applicable to systems and tools entities have previously designated as having a high or medium impact on bulk electric reliability, the WEQ CSS voted the no action recommendation during its September meeting.

1. National Institute of Standards and Technology, *Special Publication 800-63-3*, Natl. Inst. Stand. Technol. Spec. Publ. 800-63-3, 73 pages (June 2017). The finalized four-volume SP 800-63 *Digital Identity Guidelines* document suite is now available through the following link: <https://pages.nist.gov/800-63-3/>. [↑](#footnote-ref-1)
2. Exec. Order No. 13800, 82 Fed. Reg. 22391 (May 11, 2017). [↑](#footnote-ref-2)
3. Order No. 829, *Revised Critical Infrastructure Protection Reliability Standards*, 156 FERC ¶ 61, 050, 81 Fed. Reg. 49878 (2016). [↑](#footnote-ref-3)