##### August 21, 2023

**TO:** All Interested Parties

**FROM:** Elizabeth Mallett, Director, Wholesale Electric Quadrant

**RE: Cybersecurity Update**

On July 31, 2023, Version 004 of the NAESB WEQ Business Practice Standards was published and submitted to FERC in an informational filing. The new publication contains cybersecurity-related modifications in response to an informal recommendation from Sandia National Laboratories and also include revisions that respond to changing cybersecurity developments and best practices.

In a push to better support any potential industry responses to cybersecurity vulnerabilities, NAESB has compiled its existing cybersecurity-related standards into three quadrant-specific books. The new WEQ Cybersecurity book, WEQ-024, was included in the Version 004 publication. This effort was undertaken at the request of the NAESB Board of Directors and is supportive of an informal recommendation made as part of the 2019 Surety Assessment by the U.S. Department of Energy and Sandia National Laboratories. As part of that recommendation, it was suggested that NAESB consider potential methods by which the timeline for industry implementation of cybersecurity-related business practices could be expedited. As there were no new standards or material modifications made as part of this effort, NAESB was able to undertake the compilation of the RMQ, WEQ, and WGQ Cybersecurity standards through the NAESB minor correction process.

The new Version 004 publication also contains modifications to the WEQ-012 PKI Business Practice Standards, the WEQ-000 Abbreviations, Acronyms, and Definition of Terms, and the NAESB Accreditation Requirements for Authorized Certification Authorities (“ACAs”). The revised standards and specification align the standards with best industry practices regarding the issuance of server-side or transport layer security server certificates by a certificate authority and allow a NAESB ACA to issue code signing certificates which can be used to verify software and other executables in support of the NERC CIP-010 Security – Configuration Change Management and Vulnerability Assessments Reliability Standard.

Remaining to be addressed this year are efforts by the WEQ Cybersecurity Subcommittee, WEQ Business Practices Subcommittee, and RMQ Business Practices Subcommittee to review the cybersecurity protections, including the use of PKI, that may be needed to secure electronic communications for distributed energy resources. Due to the similar nature of the annual plan assignments, the WEQ and RMQ subcommittees intend to address this standards development effort jointly and are in the process of scheduling an initial kick-off meeting.