##### February 15, 2024

**TO:** All Interested Parties

**FROM:** Caroline Trum, Director, Wholesale Electric Quadrant

**RE: WEQ/RMQ/WGQ Cybersecurity Activities**

Cybersecurity is an integral element of the NAESB Business Practice Standards, and this year, the WEQ, RMQ, and WGQ will be undertaking efforts to help ensure the business practices continue to meet the cybersecurity needs of the industry. As part of the 2024 Annual Plans, the WEQ has four cybersecurity-related standards development activities. Every year, the WEQ Cybersecurity Subcommittee undertakes a proactive effort to evaluate the need for new or revised WEQ Business Practice Standards to determine if any changes are needed to meet market conditions and/or to support FERC and NERC activities related to cybersecurity. This includes a review of the current NERC Critical Infrastructure Protection Standards as well as discussion on the requirements that NAESB Authorized Certificate Authorities (ACAs) must meet in issuing digital certifications under the WEQ-012 Public Key Infrastructure (PKI) Standards as required by the NAESB Accreditation Requirements for ACAs. As noted last year, the WEQ Cybersecurity Subcommittee is also monitoring activities of the Certificate Authority/Browser (CA/B) Forum to increase the security mechanisms for PKI digital certificates. The CA/B Forum is a voluntary group comprised of certificate authorities and vendors of internet browser software that develop baseline guidance for the issuance and management of digital certificates. The subcommittee participants are evaluating the CA/B Forum’s effort to determine if any of the changes will impact how a PKI digital certificate is issued by a certificate authority or used by a certificate holder. The WEQ Cybersecurity Subcommittee plans to hold its first meeting of the year in early 2nd Quarter, 2024 to continue these discussions.

Also included as part of the 2024 WEQ Annual Plan is a joint assignment to the WEQ Cybersecurity Subcommittee and WEQ Business Practices Subcommittee (BPS) to consider and develop business practice standards for cybersecurity disclosure best practice policies, such as software supply chain risks, to support industry implementation of any applicable regulations. Additionally, last year, the WEQ Cybersecurity Subcommittee began a joint effort with the WEQ and RMQ BPS and RMQ Information Requirements/Technical Electronic Implementation Subcommittee (IR/TEIS) to review cybersecurity protections, such as PKI, that may be necessary to secure electronic communications for distributed energy resources (DERs), and develop business practices as needed. Given some of the identified timing considerations and to efficiently utilize resources, the WEQ and RMQ have elected to prioritize DER-related standards development activities in support of the U.S. Department of Energy request to NAESB in Standards Request R24001. Once completed, the subcommittees will resume consideration of cybersecurity protections to secure electronic communications for DERs and consider the development of related business practices.

Like the WEQ, the WGQ and RMQ will be meeting this year to review the WGQ Cybersecurity Related Standards Manual and RMQ Cybersecurity Model Business Practices, respectively, and revise the standards as needed. The reviews both include evaluation of the data fields identified within the standards to remove any legacy functionalities in order to limit potential cybersecurity vulnerabilities as well as an assessment of communication and encryption methodologies. The WGQ also assesses the minimum hardware and software components included within the WGQ Business Practice Standards.