##### April 23, 2024

**TO:** All Interested Parties

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

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

This year, as part of the 2024 Annual Plans, the WEQ, WGQ, and RMQ will address cybersecurity-related standard development items. Within the WEQ, the Cybersecurity Subcommittee scheduled its first meeting of the year for May 8, 2024. At this meeting, the subcommittee will begin to discuss its two individual annual plan assignments. These efforts include a review of the WEQ Business Practice Standards to evaluate the need for any modifications to meet changing market conditions or support cybersecurity-related activities by FERC and NERC as well as an assessment of the WEQ-012 Public Key Infrastructure (PKI) Business Practice Standards and the NAESB Accreditation Requirements for Authorized Certificate Authorities (ACAs), which establish the technical requirements a certificate authority must meet to become certified as a NAESB ACA. One area the WEQ Cybersecurity Subcommittee continues to monitor is activities within the Certificate Authority/Browser (CA/B) Forum to consider increased security mechanisms for PKI digital certificates. The CA/B Forum, a voluntary industry group comprised of certificate authorities and internet browser software suppliers, provides guidance on best practices to enhance internet transaction security. Some of the proposals identified for consideration could affect all PKI certificate interactions with web browsers, including those issued by NAESB ACAs. During discussions in November 2023, the WEQ Cybersecurity Subcommittee participants agreed as none of the proposals have been finalized, no immediate action is needed at this time.

Similar to the WEQ, the WGQ and RMQ also engage in a yearly review of their respective cybersecurity-related standards. These proactive efforts include an include an evaluation of the data fields identified within standards and removal of legacy functionalities to help limit potential cybersecurity vulnerabilities as well as an assessment of the communication protocols and encryption methodologies referenced within the standards. The WGQ also reviews the minimum hardware and software components identified as part of the WGQ Business Practice Standards. The WGQ and RMQ plan to convene later this year to begin addressing these annual plan items.

Beyond these activities, the WEQ and RMQ have additional cybersecurity-related standard development efforts planned for this year. First, the WEQ will be considering the development of business practice standards for cybersecurity disclosure policies to support industry implementation of any applicable regulations. This will be a joint activity between the WEQ Cybersecurity Subcommittee and the WEQ Business Practices Subcommittee. Later this year, the WEQ and RMQ plan to reconvene to continue discussions regarding cybersecurity protections necessary to secure electronic communications between distributed energy resource (DER) aggregators, utilities, and system operators. The WEQ and RMQ initiated standards development in this area in October 2023 but shifted focus earlier this year to respond to the request from the U.S. DoE to develop a standard contract for the sale and purchase of distribution services from DER aggregations. Consideration of cybersecurity related business practice standards will resume once this effort is completed.