##### August 22, 2024

**TO:** All Interested Parties

**FROM:** Amrit Nagi, Staff Attorney

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

On August 22, 2024, the WGQ and RMQ met jointly to begin the annual review of their respective cybersecurity standards. During the meeting, the participants discussed the communication protocols and encryption methodologies that are included in the standards and the identification of legacy data fields and other functionalities that could be removed to help limit potential cybersecurity vulnerabilities. The subcommittee identified minor changes that should be considered as part of the meeting and will continue discussions at the next joint meeting, scheduled for September 4, 2024 meeting.

On August 1, 2024, the WEQ Cybersecurity Subcommittee voted out a no action recommendation in support of 2024 Annual Plan Items 3.a and 3.b. The annual plan items direct the WEQ Cybersecurity Subcommittee to conduct a yearly review of the WEQ Business Practice Standards to determine if modifications are needed to address evolving market conditions or to support cybersecurity initiatives by FERC and NERC. This review includes an examination of the WEQ-012 Public Key Infrastructure (PKI) Business Practice Standards and 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. Key areas of discussion by the subcommittee included FERC Order No. 893 *Incentives for Advanced Cybersecurity Investment* and the 2024 National Security Memo on Critical Infrastructure Security and Resilience. The WEQ Cybersecurity Subcommittee also reviewed current efforts by NERC to revise its Critical Infrastructure Protection (CIP) Reliability Standards, including those that address requirements applicable to low impact bulk electric system cyber assets and virtualization. Additionally, the participants discussed the current status of activities of the Certificate Authority/Browser (CA/B) Forum to consider enhanced security measures that may impact any certificate authority issuing PKI digital certificates. While the participants have determined no additional standards development is needed at this time, the WEQ Cybersecurity Subcommittee will continue to monitor these projects.

Later this year, the WEQ and RMQ will reconvene to discuss the cybersecurity protections, including PKI, that may be needed to help secure electronic communications between distributed energy resource (DER) aggregators, utilities, and system operators. Earlier this year, following the submittal of a request from the U.S. Department of Energy, focus was shifted to the development of a NAESB standard contract to facilitate the procurement of distribution services from DER aggregations. Consideration of the cybersecurity requirements and the development of standards in this area is expected to resume once this project is complete.