##### October 8, 2025

**TO:** All Interested Parties

**FROM:** Caroline Trum, Director of Wholesale Electric Activities

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

At upcoming meetings scheduled for October 22 – 23, 2025, the Executive Committees will all consider recommendations proposing cybersecurity-related standard revisions. These recommendations, developed in response to the annual cybersecurity reviews performed by the WEQ, WGQ, and RMQ, are intended to help ensure the business practices continue to meet industry needs and support secure electronic commercial communications.

Within the WEQ, the Executive Committee will consider two recommendations. The first proposes modifications to the Accreditation Requirements for Authorized Certification Authorities (ACAs). Jurisdictional entities participating in the wholesale electric market are required by FERC to use the NAESB WEQ-012 Public Key Infrastructure (PKI) Business Practice Standards to protect certain commercial applications and market interactions through digital certificates, issued by a NAESB ACA, to encrypt data and electronically authenticate identity. The NAESB Certification Program for ACAs establishes the requirements a certificate authority must meet to become certified as a NAESB ACA and includes the Accreditation Requirements for ACAs which define the technical requirements used by NAESB ACAs to issue NAESB WEQ-012 PKI digital certificates. The revisions to the Accreditation Requirements for ACAs include the deprecation of an obsolete encryption methodology and outdated cryptographic modules used as part of digital certificate generation. These changes will help ensure NAESB ACAs continue to create and issue NAESB WEQ-012 PKI Digital Certificates in a secure manner reflective of evolving industry cybersecurity needs and are aligned with broader, general industry guidance from the National Institute of Standards and Technology and the Certificate Authority/Browser Forum regarding the issuance of PKI digital certificates. If approved, the revisions to the Accreditation Requirements for ACAs become immediately effective.

The WEQ Executive Committee will also consider a no action recommendation specific to the consideration of any impact to WEQ Business Practice Standards related to FERC and NERC cybersecurity activities. Subcommittee participants considered efforts underway by NERC to revise its Critical Infrastructure Protection (CIP) Reliability Standards as well as recent FERC action, including the Withdrawal of Notice of Inquiry and Termination of Rulemaking Potential Enhancements to the Critical Infrastructure Protection Reliability Standards in Docket No. RM20-12-000 and Order No. 907 Critical Infrastructure Protection Reliability Standard CIP-015-1 in Docket No RM24-7-000. While participants concluded that new or revised WEQ Business Practice Standards are not necessary at this time, there was agreement to continue to monitor NERC CIP-related efforts, such as those addressing third-party cloud services as well as supply chain risk management. The formal industry comment period for the recommendations concluded on September 26, 2025 with no comments received.

Both the WGQ and RMQ Executive Committees will consider recommendations proposing similar changes to their respective Cybersecurity and Quadrant Electronic Delivery Mechanism (EDM) Business Practice Standards. The proposed modifications update references to internet protocol technical guidance and create a cross-reference between the two standards manuals to better clarify that the use of both standards is necessary to help protect the electronic transmission of data. The industry formal comment periods for the WGQ and RMQ recommendations concluded on September 12, 2025 with no comments received. If approved by the respective Executive Committees and subsequently ratified by membership, the new standards will be considered final actions and included in the next version of the WGQ and RMQ Business Practice Standards.