##### April 16, 2025

**TO:** All Interested Parties

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

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

Cybersecurity protections are an integral element of the NAESB Business Practice Standards, and in recognition of their importance, the WEQ, WGQ, and RMQ each perform a yearly, proactive review of the business practices. These assessments are part of ongoing efforts by NAESB to help ensure cybersecurity elements within the standards continue to meet industry needs and support secure electronic commercial communications. Consistent with the 2025 WEQ Annual Plans, the WEQ, WGQ, and RMQ anticipate any recommendations to be presented to the Executive Committees for consideration during the October 2025 meetings.

The WEQ Cybersecurity Subcommittee will be meeting on May 7, 2025 to begin discussions in this area as part of its 2025 WEQ Annual Plan assignments. Consistent with past years, the subcommittee will discuss any changes to market conditions, recent FERC and NERC efforts in this area, and any other activities that may impact cybersecurity-related WEQ Business Practice Standards, including requirements for NAESB Authorized Certification Authorities (ACAs). Planned areas of discussion include the FERC Notice of Proposed Rulemaking (NOPR) *Supply Chain Risk Management and Reliability Standards Revisions,* which proposes the consideration of revisions to the NERC Critical Infrastructure Protection Reliability Standards related to supply chain risk management plan requirements, and recent revisions made to NERC Reliability Standards CIP-002 BES Cyber System Categorization and CIP-003 Security Management Controls. The subcommittee also will evaluate the status of efforts participants previously flagged for continued monitoring, including proposals by the Certificate Authority/Browser (CA/B) Forum that could affect how web browsers interact with PKI digital certificates, like those issued by NAESB ACAs. The CA/B Forum is an industry group of digital certificate authorities and internet browser software suppliers that provides guidance on best practices to enhance the security of internet transactions.

Like the WEQ, the WGQ and RMQ are planning to meet later this year to review the cybersecurity elements within the WGQ Cybersecurity Related Standards Manual and RMQ Cybersecurity Model Business Practices, respectively. This review includes an assessment of the communication and encryption methodologies used to secure the electronic transmission of data and protect browser-based transactions as well as the identification and removal of legacy functionalities to help mitigate potential cybersecurity vulnerabilities. The WGQ also considers if revisions are needed to the minimum hardware and software components identified within the business practices. These minimum components include operating systems requirements and versioning of supported internet browsers and related plug-ins utilized in the development and maintenance of Informational Posting and Customer Activities Web sites maintained by interstate natural gas pipelines.