##### August 18, 2021

**TO:** All Interested Parties

**FROM:** Caroline Trum, NAESB Deputy Director

**RE: Update to the Board of Directors – WGQ/WEQ/RMQ Cybersecurity Activities**

Through Orders No. 676-J and 587-Z, the FERC has taken action to incorporate by reference the wholesale electric and wholesale gas cybersecurity related business practice standards developed by NAESB to address Sandia National Laboratories’ recommendations to mitigate potential security issues made as part of the 2019 Surety Assessment sponsored by the U.S. Department of Energy. In response to the recommendations, NAESB developed WEQ, WGQ, and RMQ Business Practice Standards that serve to strengthen the practices and cybersecurity protections established through the standards by aligning security requirements with other cybersecurity guidelines, mitigating potential vulnerabilities, and incorporating more secure communication and encryption methodologies. The WEQ cybersecurity related standards were included as part of an informational filing made by NAESB with the FERC in March 2020 regarding WEQ Version 003.3 and the subject of a NOPR released in July 2020. The WGQ cybersecurity related standards were included as part of an informational filing made by NAESB with the FERC in August 2020 regarding WGQ Version 3.2 and the subject of a NOPR released in February 2021. The RMQ Business Practice Standards have been made available to state commissions through the National Association of Regulatory Utility Commissioners.

This year the WEQ Cybersecurity Subcommittee and WGQ Electronic Delivery Mechanism (EDM) Subcommittee have been meeting to discuss cybersecurity related issues and any actions that may need to be taken to revise the existing standards. In July, the WEQ Cybersecurity Subcommittee voted out a recommendation proposing modifications to the NAESB Accreditation Requirements for Authorized Certification Authorities (ACAs) that will establish requirements for NAESB ACAs issuing code signing certificates. As recognized by the subcommittee participants, there is a growing reliance on the use of code signing certificates to verify software and other executables, and these revisions will be supportive the NERC CIP-010 Cyber Security – Configuration Change Management and Vulnerability Assessment Reliability Standards which require verification of the identity of a software source. In developing the recommendation, the WEQ Cybersecurity Subcommittee reviewed the existing NERC CIP Standards, the NERC projects under development that could result in modifications to the NERC CIP Standards, the FERC *Potential Enhancements to the Critical Infrastructure Protection Reliability Standards Notice of Inquiry*, the FERC *Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security Notice of Inquiry*, and the May 12, 2021 *Executive Order on Improving the Nation’s Cybersecurity*. Additionally, the WEQ Cybersecurity Subcommittee also voted out a recommendation proposing minor changes to the WEQ-012 Public Key Infrastructure Business Practice Standards to ensure consistency in the use of defined terms, abbreviations, and acronyms. Both recommendations will be considered by the WEQ Executive Committee during its meeting on October 5.

The WGQ EDM Subcommittee held a meeting on June 17 to discuss the May 12, 2021 *Executive Order on Improving the Nation’s Cybersecurity.* The subcommittee will also be meeting jointly this year with the RMQ Information Requirements and Technical Electronic Implementation Subcommittee to review the WGQ/RMQ Internet Electronic Transport Business Practice Standards to identify and remove any legacy functionalities in order to limit potential cybersecurity vulnerabilities.