##### February 21, 2023

**TO:** All Interested Parties

**FROM:** Elizabeth Mallett, Director, Wholesale Gas Quadrant and Retail Markets Quadrant

**RE: Cybersecurity Update**

During the March Executive Committee meetings, each quadrant will consider the cybersecurity items related to the integration of Multi-Factor Authentication (MFA) into the standards and also the recommendations developed in response to standing annual plan items to review the standards for cybersecurity updates. Additionally, the WGQ and RMQ Executive Committees will consider the compilation of the new RMQ and WGQ cybersecurity books.

Multi-Factor Authentication

On March 10th, the thirty-day formal comment periods will conclude for three recommendations that address whether baseline Multi-Factor Authentication (MFA) should be integrated into the NAESB standards. During its March meeting, the WEQ Cybersecurity Subcommittee (CSS) developed a no action recommendation in response to this item. The WEQ CSS explained that the standards already incorporate MFA through the utilization of PKI digital certificates. Beyond the use of PKI digital certificates, the OASIS standards currently require two-factor client authentication in controlling access to an OASIS node, and the NAESB Electronic Tagging Functional Specification requires the additional use of security keys to authenticate an entity involved in the e-Tag messaging system. The WGQ and RMQ held joint meetings to develop recommendations concerning Multi-Factor Authentication. The RMQ IR/TEIS voted out a no action recommendation in response to the item because the standards do not address that area. In the WGQ, the WGQ EDM Subcommittee developed and approved a recommendation to modify four WGQ Quadrant Electronic Delivery Mechanisms (QEDM) Related Standards. As stated above, all three recommendations will be considered during the respective Executive Committee meetings this March.

Compilation of New Cybersecurity Books

The RMQ and WGQ have approved recommendations addressing minor corrections that move existing cybersecurity-related business practices into a new suite of NAESB Business Practice Standards for each quadrant. These activities support the direction from the NAESB Board of Directors to address an informal recommendation made by Sandia National Laboratories. That recommendation asked that NAESB, working with FERC, consider methods to abbreviate the timeline for industry implementation of cybersecurity-related business practice standards. The minor corrections will be discussed during the March RMQ and WGQ Executive Committee meetings. As you may remember, the WEQ completed their compilation of the WEQ Cybersecurity Business Practice Standards at the end of last year. The creation of the new books will be reflected in Version 003.4 of the WEQ Business Practice Standards, Version 3.4 of the RMQ Model Business Practices, and Version 3.3 of the NAESB WGQ Business Practice Standards which are anticipated to be published next year.

Annual Reviews

The WGQ and RMQ are working together to undertake an annual review to determine if any modifications or additions regarding cybersecurity elements are needed. As part of this effort, the WGQ EDM and RMQ Information Requirements/Technical Electronic Implementation Subcommittee (IR/TEIS) will hold joint meetings to review the data used in the WGQ Internet Electronic Transport specification for data fields that may no longer be utilized and determine if these data fields can be removed.A review of the minimum technical characteristics in the Appendices of the WGQ QEDM Manual will be conducted to determine whether any changes are appropriate. On the WEQ side, the WEQ CSS annual review of the WEQ-012 Public Key Infrastructure Business Practice Standards and the accreditation requirements for Authorized Certification Authorities to determine if any changes are needed to meet market conditions resulted in a no action recommendation. The WEQ CSS also voted out a no action recommendation after evaluating whether any modifications to the NAESB Business Practice Standards are needed to support the current version of the NERC Critical Infrastructure Protection Standards and any other activities of NERC and the FERC related to cybersecurity.