##### December 12, 2023

**TO:** All Interested Parties

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

**RE: Cybersecurity Update**

This year, NAESB prioritized numerous standards development activities to maintain secure electronic communications for the gas and electric industries. In a push to better support any potential industry responses to cybersecurity vulnerabilities, NAESB compiled its existing cybersecurity-related standards into three quadrant-specific books. This effort was undertaken at the request of the NAESB Board of Directors and is supportive of an informal recommendation made as part of the 2019 Surety Assessment by the U.S. Department of Energy and Sandia National Laboratories. As part of that recommendation, it was suggested that NAESB consider potential methods by which the timeline for industry implementation of cybersecurity-related business practices could be expedited. As there were no new standards or material modifications made as part of this effort, NAESB was able to undertake the compilation of the RMQ, WEQ, and WGQ Cybersecurity standards through the NAESB minor correction process.

In July, Version 004 of the NAESB WEQ Business Practice Standards were published and an informational filing was submitted to the Federal Energy Regulatory Commission. The new publication contained the cybersecurity-related modifications not only in response to the informal recommendation from Sandia, but also revisions that respond to changing cybersecurity developments and best practices regarding the issuance of server-side or transport layer security server certificates by a certificate authority. Further, the revised standards allow a NAESB ACA to issue code signing certificates which can be used to verify software and other executables in support of the NERC CIP-010 Security – Configuration Change Management and Vulnerability Assessments Reliability Standard.

Additionally, Version 4.0 of the NAESB WGQ Business Practice Standards were published at the end of September and were included in an informational filing to FERC. The standards strengthen the authentication processes used in identification verification for commercial transactions within the wholesale natural gas market by supporting the use of multi-factor authentication and encouraging the use of whitelisting by market participants for file-to-file transactions, such as those conducted via Electronic Data Interchange (EDI)/EDM and Flat File (FF)/EDM.

During a November meeting, the WEQ Cybersecurity Subcommittee (CSS) heard a presentation from Lila Kee of GlobalSign concerning potential changes to requirements for NAESB ACAs issuing NAESB PKI digital certificates. The NAESB Accreditation Requirements for ACAs requires alignment with certain Certificate Authority/Browser (CA/B) Forum guidance. The CA/B Forum is now considering proposed changes to its guidance that, if implemented, could impact how NAESB ACAs issue NAESB digital certificates and how those certificates are used by NAESB end entities. During its November meeting, the WEQ CSS noted that the proposals discussed by the CA/B Forum have not been finalized; however, the WEQ CSS will to continue to evaluate the status of the proposals as part of the annual plan item discussions regarding market changes or trends that could necessitate changes to the WEQ-012 PKI Business Practice Standards and the NAESB Accreditation Requirements for ACAs.

On December 1st, the NAESB Board Certification Program Committee approved non substantive modifications to the NAESB Authorized Certification Authority Process via a notational ballot distributed in mid-November. The modifications, prompted through discussion during a November WEQ CSS meeting, revise the Section 5 Compliance with WEQ-012 Requirements to identify the standards that are secured under the NAESB WEQ-012 Public Key Infrastructure (PKI) Business Practice Standards.

Looking ahead to next year, the WEQ Cybersecurity Subcommittee, WEQ Business Practices Subcommittee, and RMQ Business Practices Subcommittee will continue to discuss cybersecurity protections, including PKI, that may be needed to secure electronic communications for distributed energy resources. Additionally, the 2024 quadrant annual plans contain cybersecurity items.