##### November 17, 2021

**TO:** All Interested Parties

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

**RE: Cybersecurity Update**

Over several of its past meetings, the NAESB Board Strategy Committee has been discussing an informal recommendation made by Sandia National Laboratories as part of the 2019 Surety Assessment, that NAESB, working with the U.S. Department of Energy and FERC, consider how the industry could expediate the process by which cybersecurity related standards are developed, adopted, and implemented. In discussions, the committee identified several proposals NAESB could consider undertaking, including maintaining all cybersecurity related requirements within a single suite of standards for each quadrant, developing cybersecurity related specifications for each quadrant, and/or establishing a certification program to specifically support the cybersecurity related standards. At the request of the committee, on October 21, NAESB distributed a survey to members of the NAESB Board of Directors and Advisory Council to solicit feedback on the proposals and input on any other options that should be considered. Survey responses were due on November 11. The NAESB Board Strategy Committee will be meeting on November 30 to discuss the results and prepare a recommendation for consideration to the NAESB Board of Directors on how to proceed.

As part of its October 5 meeting, the WEQ Executive Committee approved two recommendations developed by the WEQ Cybersecurity Subcommittee. The first recommendation proposed modifications to the *NAESB Accreditation Requirements for Authorized Certification Authorities* (ACAs), which supports the NAESB Certification Program for ACAs by establishing the technical requirements a certificate authority must meet in issuing a digital certificate. The revisions incorporate requirements that must be followed in the issuance of code signing certificates, which are used to verify the origination of software, applications, and other executables. The changes are also supportive of requirements in the NERC CIP-010 the NERC CIP-010 Cyber Security – Configuration Change Management and Vulnerability Assessment Reliability Standards that require verification of the identity of a software source. The new version of the *NAESB Accreditation Requirements for ACAs* became effective upon the approval of the WEQ Executive Committee.

Additionally, the WEQ Executive Committee approved a recommendation proposing modifications to the WEQ-012 Public Key Infrastructure (PKI) Business Practice Standards. The recommendation made minor, non-substantive revisions to ensure consistency in the use of defined terms, abbreviations, and acronyms. The standards were ratified by WEQ membership on November 4 and will be incorporated into the next version of the WEQ publication.

The WEQ, WGQ, and RMQ all have cybersecurity related items included as part of the proposed 2022 Annual Plans to be presented to the NAESB Board of Directors for approval during its December 9 meeting. For the WEQ, these including standing items assigned to the WEQ Cybersecurity Subcommittee to assess the WEQ-012 PKI Business Practice Standards and the *NAESB Accreditation Requirements for ACAs* and make any necessary modifications to meet changing market conditions as well as evaluate the NERC CIP Reliability Standards and any other NERC or FERC cybersecurity-related activities and develop supporting and/or complementary business practices as needed. As part of 2021 standard development efforts, the WEQ Cybersecurity Subcommittee has identified several items to review in 2022 that could result in modifications to the NERC CIP Reliability Standards, including NERC Project 2020-04 Modifications to CIP-012 and NERC Project 2021-03 CIP-002 Transmission Owner Control Centers. Within the WGQ and RMQ, the WGQ Electronic Delivery Mechanism (EDM) and RMQ Information Requirements/Technical Electronic Implementation Subcommittee (IR/TEIS) have been jointly assigned an item on the proposed 2022 WGQ and RMQ Annual Plans to review the WGQ and RMQ Internet Electronic Transport Business Practice Standards and identify and eliminate any legacy data that may no longer be utilized.