##### November 30, 2020

**TO:** All Interested Parties

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

**RE: Cybersecurity Update**

This year, NAESB has undertaken several standard development efforts related to cybersecurity. Most notably, NAESB has now completed all standard development activities identified to respond to the surety assessment performed by Sandia National Laboratories.

On November 16, 2020, the formal comment period closed for recommendations developed by the WGQ Electric Delivery Mechanism (EDM) Subcommittee and the RMQ Information Requirements/Technical Electronic Implementation Subcommittee (IR/TEIS) proposing modifications to the WGQ and RMQ Internet Electronic Transport Business Practice Standards. With these recommendations, the WGQ and RMQ have addressed all assigned standard development efforts in response to the Sandia National Laboratories surety assessment. The recommendations will be considered by the WGQ and RMQ Executive Committees during their next meetings.

In October, the WEQ Executive Committee adopted a no action recommendation developed by the WEQ Cybersecurity Subcommittee to address the remaining additional findings identified by Sandia National Laboratories as part of the surety assessment and assigned to the WEQ for standards development consideration. Through subcommittee discussions, including a joint meeting with the WEQ OASIS Subcommittee, a determination was made that the issues presented by the additional findings were either already addressed by existing requirements in the WEQ Business Practice Standards, the NAESB Accreditation Requirements for Authorized Certification Authorities, and the ACA Process or were not applicable to the processes and communication protocols utilized within the WEQ standards.

During the September 3, 2020 meeting, the NAESB Board of Directors adopted a report developed by the Board Critical Infrastructure Committee that described the efforts of the WEQ, WGQ, and RMQ to respond to the recommendations of the surety assessment. As done in the past, this report was provided to the DoE and Sandia National Laboratories. At the request of the Department of Energy, NAESB expediated standard development efforts to address the potential security issues identified by Sandia National Laboratories. Within seven months of receiving the surety assessment reports, NAESB completed the standards development efforts to mitigate the potential security issues. These standard modifications support the use of industry cybersecurity best practices, remove legacy functionality that could potentially provide a vehicle for cyber-attacks, and incorporate more secure communication protocols and encryption methodologies. The new and revised standards were incorporated into new publications of the RMQ Model Business Practices, the WEQ Business Practice Standards, and the WGQ Business Practice Standards, all published earlier this year.

After the publication of Version 003.3 of the WEQ Business Practice Standards and Version 3.2 of the WGQ Business Practice Standards, NAESB made an informational filing regarding the new standards with the FERC that contained high-level descriptions of the standards modifications, including the cybersecurity related changes. NAESB submitted the WEQ-related filing on March 30 and the WGQ-related filing on August 15. On July 16, the FERC issued a Notice of Proposed Rulemaking (NOPR) that proposed to incorporate by reference, with few exceptions, Version 003.3 of the WEQ Business Practice Standards. The proposal includes all cybersecurity-related modifications NAESB made to the WEQ Business Practice Standards in response to the recommendations made by Sandia National Laboratories. The comment period for the NOPR closed on November 3, 2020.

In 2017, NAESB announced that Sandia National Laboratories, through funding provided by the U.S. Department of Energy (DoE), would be performing a surety assessment to analyze cybersecurity elements within the NAESB Business Practice Standards. NAESB worked closely with Sandia National Laboratories and representatives from the U.S. DoE throughout the surety assessment process, and on July 22, 2019, Sandia National Laboratories provided NAESB with the surety assessment reports: (1) Assessment Report of the NAESB Public Key Infrastructure Program; (2) Assessment Report of the NAESB OASIS Standards; (3) Assessment Report of the NAESB Business Operations Practices and Standards; and (4) Addendum Report: Threat-based Examination of NAESB Standards and Business Operations. Within these reports, Sandia National Laboratories identified six potential security issues and provided recommendations to mitigate each identified issue. Additionally, the reports contained twenty-two additional findings made by Sandia National Laboratories for further consideration by NAESB.