##### February 25, 2020

**TO:** All Interested Parties

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

**RE: Update on Sandia National Laboratories Surety Assessment**

In April 2017, NAESB announced that Sandia National Laboratories would be performing a surety assessment on the NAESB Business Practice Standards sponsored by the Department of Energy. Sandia National Laboratories has performed two previous surety assessments on the NAESB Business Practice Standards with recommendations from these assessments resulting in modifications to the standards. The purpose of the current surety assessment is to analyze cybersecurity elements within the NAESB Business Practice Standards and focuses on four areas: (1) assess the NAESB Certification Program for Accredited Certification Authorities, including the Wholesale Electric Quadrant Public Key Infrastructure Standards, the NAESB Accreditation Requirements for Authorized Certificate Authorities, and the Authorized Certification Authority Process; (2) assess the Wholesale Electric Quadrant OASIS Suite of Business Practice Standards; (3) assess the Wholesale Gas Quadrant and Retail Market Quadrant Internet Electronic Transport and Electronic Delivery Mechanism Standards; and (4) conduct a high-level dependency analysis between the gas and electric markets.

On July 22, 2019, Sandia National Laboratories provided NAESB with the final surety assessment reports. There are four reports in total: (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. In total across the four reports, Sandia National Laboratories made twelve recommendations to mitigate security issues and identified twenty-two additional findings or considerations. To help meet the request by the Department of Energy that, where possible, NAESB expediate any standards development efforts resulting from the surety assessment, the Board Critical Infrastructure Committee held two meetings in August to review the reports and provide context to the assigned standard development items.

During the February 18, 2020 WEQ Executive Committee, the committee adopted WEQ standards that were assigned individually to the WEQ Cybersecurity Subcommittee and the WEQ OASIS Subcommittee and several items that were jointly assigned to both subcommittees. Both subcommittees held a series of meetings, both separate and joint, to address the assigned standard development efforts. On October 3, the WEQ OASIS Subcommittee and WEQ Cybersecurity Subcommittee jointly voted out a recommendation proposing modifications to the WEQ OASIS Suite of Business Practice Standards to address all jointly assigned security issues and additional findings or considerations. In total, the recommendation proposes modifications to fourteen standards: WEQ-001-13.1.3, WEQ-002-2.3, WEQ-002-2.4, WEQ-002-4.2.1.2, WEQ-002-4.2.1.3, WEQ-002-4.2.2, WEQ-002-5, WEQ-002-5.1.1, WEQ-002-5.1.2, WEQ-002-5.1.3, WEQ-002-5.6, WEQ-002-101.2.3.1, WEQ-002-101.3.3.2, and WEQ-002-101.3.3.3. These revisions remove legacy functionality, update the minimum encryption and security protocols, and revise implementation requirements to incorporate industry best practices for areas such as software/hardware patching, business continuity and disaster recovery exercises, firewalls, and password management and authentication. Once ratified by NAESB membership, the standards will be incorporated into Version 3.3 of the WEQ Business Practice Standards.

Also on February 18, the WEQ Executive Committee approved modifications to the NAESB Accreditation Requirements for Authorized Certification Authorities. The recommendation containing the modifications was voted out of the WEQ Cybersecurity Subcommittee on October 10 and proposes modifications to address remaining assigned security issues and several of the assigned additional findings or considerations. The recommendation proposes modifications to seven requirements: Section 1 – Introduction, Section 5.1.1 – Certificate Authority Key Pair Generation, Section 5.1.2 – Subscriber Key Pair Generation, Section 5.1.6 – Key Sizes, Section 5.1.7 – Public Key Parameters Generation and Quality Checking, Section 5.2.1 – Cryptographic Module Specifications and Controls, and Section 5.2.7 – Private Key Storage on Cryptographic Module. Among other changes, the revisions modify key lengths and encryption methods to reflect current industry guidelines and best practices, remove legacy functionality, and update references to the most recent Federal Information Processing Standards Security Requirements for Cryptographic Models. The new version of the NAESB Accreditation Requirements for Authorized Certification Authorities is now effective and available on the NAESB website.

The standard development efforts applicable to the RMQ and WGQ were jointly assigned to the RMQ Information Requirements and Technical Electronic Implementation Subcommittee (IR/TEIS) and the WGQ Electronic Delivery Mechanism (EDM) Subcommittee. The subcommittees held a series of joint meetings from August through December 2019 to review assigned items and develop recommendations. The recommendations in response to the surety assessment were reviewed and approved during the February 20, 2020 WGQ Executive Committee meeting and via a notational ballot to the RMQ on December 20, 2019.

On December 2, 2019, the RMQ IR/TEIS voted out a recommendation proposing modifications to the RMQ EDM and Internet Electronic Transport (IET) Model Business Practices. In total, the recommendation proposes modifications or reservations to eighteen model business practices: RMQ.5.3.2.2, RMQ.5.3.4.14, RMQ.7.1.7, RMQ.7.1.9, RMQ.7.2.33, RMQ.7.2.34, RMQ.7.3.4, RMQ.7.3.15, RMQ.7.3.16, RMQ.7.3.25, RMQ.7.1.33, RMQ.10.1.7, RMQ.10.2.33, RMQ.10.2.34, RMQ.10.3.4, RMQ.10.3.15, RMQ.10.3.16, and RMQ.10.3.25. Modifications were also proposed to Appendices A and B of the RMQ IET Model Business Practices. Additionally, four new standards were proposed. Among other changes, the revisions serve to establish timelines for the adoption of security patches and the notification to trading partners of security related issues, to incorporate specific and broad adoption of system security measures, to eliminate legacy functionality, and to update key and encryption methodologies. The RMQ Executive Committee acted to adopt the recommendation during its meeting on December 18, 2019. RMQ membership ratified the revisions on January 17, 2020, and the model business practices were incorporated into RMQ Version 3.3 published on January 30, 2020.

On December 2, 2019, the WGQ EDM Subcommittee voted out the recommendation proposing modifications to the WGQ EDM and IET Business Practice Standards to address the assigned security issues and several of the assigned additional findings or considerations. The subcommittee voted out a subsequent recommendation on January 21, 2020 proposing additional modifications to the WGQ EDM Business Practice Standards. Together, these recommendations propose modifications or reservations to fourteen standards: WGQ Standard Nos. 4.1.15, 4.1.39, 4.3.60, 4.3.61, 4.3.83, 4.3.84, 10.1.7, 10.1.9, 10.2.33, 10.2.34, 10.3.4, 10.3.15, 10.3.16, and 10.3.25. Modifications were also proposed to Appendices A – D of the WGQ EDM Business Practice Standards and Appendices A and B of the WGQ IET Business Practice Standards. Additionally, four new standards were proposed. Similar to the changes made by the RMQ, these revisions establish timelines for the adoption of security patches and the notification to trading partners of security related issues, to incorporate specific and broad adoption of system security measures, to eliminate legacy functionality, and to update key and encryption methodologies. Once ratified by the NAESB membership, the standards will be incorporated into Version 3.2 of the WGQ Business Practice Standards. The WGQ EDM Subcommittee will reconvene later this year to address the remaining assigned additional findings or considerations, including topics covering REFNUM and whitelisting.

On February 28, the Board Critical Infrastructure Committee will meet to prepare a report, similar to the report following the 2006 surety assessment. Through the report, NAESN will inform the Department of Energy and Sandia National Laboratories of the NAESB efforts to address the findings and recommendations in the 2019 surety assessment.