North American Energy Standards Board

801 Travis, Suite 1675, Houston, Texas 77002
Phone: (713) 356-0060, Fax: (713) 356-0067, E-mail: naesb@naesb.org
Home Page: www.naesb.org

via email

December 7, 2018

Benjamin Anderson
Sandia National Laboratories
PO Box 5800
Albuquerque, NM 87185

RE: Surety Assessment Draft Outline

Dear Mr. Anderson,

NAESB would like to express thanks to you and your team at Sandia National Laboratories for providing the opportunity to review the surety assessment draft reports provided in November. The NAESB Critical Infrastructure Committee met on December 3, 2018, and this document serves as the written feedback of the committee regarding the latest draft reports. In general, the committee noted that the incorporated revisions appear to be responsive to some of the previous feedback provided to Sandia National Laboratories in August; however, while the current reports contain valuable information that may assist the industry at large, the resulting analyses are generalized and contain broad recommendations that could be subject to interpretation and prove difficult to translate to standards development. Additional granularity through more detailed analyses and specific, recommended actions are needed to equip NAESB with the necessary information to assess the need for additional standards development to incorporate any recommended cybersecurity best practices addressing the current and future needs of the wholesale and retail gas and electric markets. To assist Sandia National Laboratories in the development of the final reports are considerations from the NAESB Critical Infrastructure Committee:

1. Regarding the Assessment Report of the North American Energy Standards Board Public Key Infrastructure Program (PKI Report), the committee requested analysis of any known or potential future vulnerabilities with the use of an X.509 digital certificate and if such vulnerabilities exist, specific actions that can be carried out through standard modifications and/or additions for mitigation.

2. Additionally, within the PKI Report, the committee noted that the conclusion of the report did not contain a description of the attack vector(s) that could be exploited as a result of an out of compliance NAESB Authorized Certificate Authority. The committee recommended the conclusion of this report be revised to contain more details or provide a clearer analysis.

3. Regarding the Assessment Report of the North American Energy Standards Board Open Access Same-Time Information Systems (OASIS) Standards (OASIS Standards Report), the committee appreciated the inclusion of these standards in the assessment as there have been many changes in the cybersecurity landscape since their original drafting; however, the resulting analysis only contained recommendations to continue to engage with the industry and the Federal Energy Regulatory Commission (FERC) or generalized categories for best practices for the industry to consider. One such best practice consideration was the encryption of all communications (as allowable). The committee questioned if there were any specific recommended actions NAESB should consider, such as the expansion of Public Key Infrastructure or the type and level of encryption.

4. From comments submitted by committee members outside of the meeting, there was also a request that within the OASIS Standards Report, Sandia National Laboratories provide an analysis of any potential risks associated with areas of constraint that could be used in attack vectors and any actions to shore up business processes that could mitigate such risks.

5. Regarding the Assessment Report of the North American Energy Standards Board Business Operations Practices and Standards (Business Operations Practices and Standards Report), the committee stated a need for additional details in the resulting recommendations. Regarding the recommendation as part of Section 6.1.1, due to the potential for the wholesale gas and electric standards to be acted upon by the FERC through the incorporation by reference process as well as compatibility and security considerations, it is not always

practical for the NAESB Business Practice Standards to reference the latest version of a technology or protocol in lieu of a specific version. Of greater benefit would be a listing of suggested minimum versioning for each technology and protocol currently incorporated into the standards and descriptions of the risks/justifications for those minimum versioning recommendations.

6. Further, an identification of all the legacy, deprecated, or rarely used functionalities considered as part of Section 6.1.2 of the Business Operations Practices and Standards Report would provide NAESB a starting point for future review as recommended by Sandia National Laboratories.

7. Another observation of the committee regarding the Business Operations Practices and Standards Report was the recommendation that when moving towards autonomous systems, there be a consideration of the strength of human control in preventing/detecting abnormal behavior. The committee requested the final report include specific, recommended human actions/points of oversight and an identification of the areas in in the process that could benefit from human monitoring.

8. Regarding the Comments on the EDI Cyber Attack, the committee suggested incorporating the discussion into one of the other reports. Although the comments provide value, due to the lack of publicly available information and any specific recommended actions to mitigate vulnerabilities, a separate report may not be warranted.

9. Regarding the Addendum Report: Threat-based Examination of NAESB Standards and Business Operations, the committee noted the benefit in the final report providing detailed information about the most likely types of potential cyberattacks faced by the industry, specifically those impacting control and/or operation systems, and actionable recommendations to mitigate. Of particular interest would be the convergence of information technology (IT) systems and operational technology (OT) systems, any known or potential future vulnerabilities, and steps for risk mitigation that could be addressed through new or modified business practice standards.

10. Several of the draft reports suggested reporting metrics by the industry to NAESB following a cyber-attack. While these metrics could provide important information to the industry regarding potential considerations in the aftermath of an attack, NAESB is not involved in any aspects of compliance or compliance monitoring. Instead, the committee requested Sandia National Laboratories provide recommendations that speak to the reporting processes and minimum information entities should make available to other entities, such as trading partners, customers, or regulators, following a cyber-attack.

11. The committee noted that the draft reports did not address tools or technologies that could present opportunities for future exploitation. As in the previous feedback, the committee requested the final reports provide an evaluation of emerging technology and trends, including real-time data transfers, the use of cloud technology, increased OT/IT connections, blockchain, and mobility. An analysis that identified potential future areas of vulnerability and made concrete recommendations for how to protect against that risk, such as the level of encryption, a specific encryption protocol, or human involvement would provide the basis to consider forward-thinking standards development.

12. Based on additional comments submitted outside the meeting, committee members also requested the final reports contain analysis comparing the cybersecurity protocols utilized within the Wholesale Electric Quadrant Standards (PKI) and the Wholesale Gas Quadrant and Retail Markets Quadrant Standards (PGP). A main purpose of the surety assessment is to conduct a high-level dependency analysis between the gas and electric markets. Given the increasing levels of interaction and harmonization between the gas and electric industries, the final report should discuss any inconsistencies or gaps related to cybersecurity between the markets and recommend actions to resolve any identified issues.

13. Finally, aligned with the vulnerability-based analysis previously requested by the committee, it would be helpful if the final reports contained a detailed listing or table of each requirement within the applicable

801 Travis, Suite 1675, Houston, Texas 77002
Phone: (713) 356-0060, Fax: (713) 356-0067, E-mail: naesb@naesb.org
Home Page: www.naesb.org

standards, identified if that requirement meets security goals or represents a risk and if so, provides a recommended action and timeframe for mitigation.

As illustrated by the above comments of the NAESB Critical Infrastructure Committee and described in previous feedback, the final reports should contain the identification of any standard or requirement that may represent a risk, a clear explanation of that risk, and a granular recommendation for specific changes or improvements to the standards that should be considered for mitigation purposes. It is our understanding that additional commentary on the draft reports is forthcoming from the National Institute of Standards and Technology and will be forwarded to you and your team as soon as it is received. A final report incorporating these considerations will provide NAESB with the necessary basis to quickly determine any standards development efforts that should be undertaken and enact those changes.

NAESB appreciates the efforts of both the Department of Energy and Sandia National Laboratories regarding the surety assessment and looks forward to receiving the final reports.

Best Regards,

J. Cade Burks
Co-Chair, NAESB Critical Infrastructure Committee

David Darnell,
Co-Chair, NAESB Critical Infrastructure Committee

cc: Ms. Rae McQuade, President & COO, North American Energy Standards Board
Mr. Michael Desselle, Chairman & CEO, North American Energy Standards Board
Mr. William P. Boswell, General Counsel, North American Energy Standards Board
Mr. Jonathan Booe, Executive Vice President & CAO, North American Energy Standards Board