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

March 20, 2018

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

RE: Surety Assessment Draft Outline

Dear Mr. Anderson,

NAESB appreciates the opportunity to review the draft report of the results of the surety assessment performed by you and your colleagues and to provide feedback prior to the finalization of the report. By performing an analysis of the NAESB Wholesale Gas, Wholesale Electric, and Retail Markets business practice standards and Public Key Infrastructure Program to identify any potential areas presenting security concerns and making recommendations to address these concerns, Sandia National Laboratories is ensuring that the energy markets employ the best practices to strengthen cybersecurity. Further, the dependency analysis between the gas and electric markets to identify potential vulnerabilities that could be used to leverage cross-market attacks will help safeguard the energy markets as there is increased use of gas for power generation. In response to the submittal of the draft report, the NAESB Critical Infrastructure Committee met on February 26, 2018 to review and discuss the draft as well as provide feedback regarding the finalization of the report. While the committee agreed that the draft report provides an outline that will serve as a solid foundation upon which the finalized report can be developed, a number of questions and concerns were raised and have been included below to assist Sandia National Laboratories in the development of the final report:

1. Provide a Sandia National Laboratories report similar in structure and format to past reports. Following the Sandia National Laboratories surety assessment conducted in 2006, the report provided to NAESB contained in-depth detail about the research conducted and provided a comprehensive assessment that included informative findings and definitive recommendations. The findings and recommendations were supported by thorough analyses and included critical success factors and metrics. A final report structured in a similar manner with findings, recommendations, and analyses will be valuable to NAESB as it reviews the results of the surety assessment and determines next steps.
2. Provide specific details, analyses, and recommendations on the standards considered as part of the surety assessment. In reviewing the draft report, the NAESB Critical Infrastructure Committee recognized a need for the final report to contain a level of detailed specificity. The committee appreciates that Sandia National Laboratories considered the elements necessary to conduct the assessment; however, the draft report does not provide the surety that is expected by NAESB membership on the adequacy of the current NAESB standards. Generalized statements on the complexities of the interactions of the gas and electric markets do not provide the specific requirements needed by NAESB membership. It is necessary for the report to provide the specific standards and security measures addressed as part of the surety assessment and a detailed analysis on their adequacy in protecting against current and future cyber threats. This would include detailed documentation on the review and analysis of the current security and encryption procedures for all electronic data communications. While not a complete list of considerations, two such examples would be the use of digital signatures and Secure Socket Layer (SSL) encryption.
3. Provide specific information on any potential gaps or vulnerabilities found while conducting the surety assessment. The report provided to NAESB following the 2006 surety assessment contained discussion on potential gaps or deficiencies, characterized the potential nature of cyber-attacks, described how vulnerabilities could be exploited, and made recommendations for mitigation. The NAESB Critical Infrastructure Committee identified this type of information as helpful to NAESB following the previous surety assessments to ensure the standards continued to provide adequate cybersecurity.
4. Describe the scenarios considered as part of the surety assessment, including specific scenarios identified below, and potential consequences of a cyber-attack including economic and potential reliability

considerations. During the meeting of the NAESB Critical Infrastructure Committee, several examples were provided of concerns not included in the draft report. Based on the information in the draft report, the committee was unsure as to whether or not these issues or scenarios were considered as no justification was provided for their exclusion. Several different topics were discussed, with specific examples noted by committee members. This is not an exhaustive list, and it would be useful to NAESB if these and the various scenarios also considered by Sandia National Laboratories while conducting the surety assessment were explained in the final report.

a. Situations where capacity is maliciously overbooked on a pipeline, causing those needing natural gas to seek pipeline capacity from elsewhere, such as storage or the sport market, potentially creating an artificial market and causing inflated pricing that could ultimately result in higher costs being passed onto the consumer. This scenario could greatly affect the intra-day market and those offering hourly services.
b. The consequences beyond monetary disputes between parties that may arise from a cross-market attack. For example, through automatic flow control, pipelines control the flow of gas through a meter between a pipeline and the gas-fired generation facility. Should a nomination from a gas-fired generation facility be nefariously prevented from being delivered to a pipeline, gas may not flow to the specific facility in question. This will likely either prevent the facility from starting-up or force the facility to shut-down. Likewise, malicious alterations to a nomination may cause a gas-fired generation facility to overtake, which could cause a pipeline to halt the flow of gas to the gas-fired generation facility, resulting in a similar outcome. In either situation, as the gas-fired generation facility would not be producing the anticipated electric generation, this could cause reliability issues on the electric grid. Further, if the gas-fired generation facility is started up without flowing gas, the facility could be damaged and require a lengthy repair period which might also contribute to reliability issues on the electric grid. Any malicious changes to gas nominations with an intended delivery point(s) to gas-fired generation facilities ultimately have the capability to impact the electric grid's reliability.

NAESB values our working relationship with the Department of Energy and Sandia National Laboratories through the Office of Oil and Natural Gas sponsorship of this third surety assessment project. We are hopeful that the finalized report, with the modifications requested above, will provide valuable information to NAESB that the industry can utilize to ensure the NAESB business practice standards continue to provide reliable protections against cyber threats. As explained above, a detail-centric final report that builds on the high-level outline provided in the draft report will assist NAESB membership in the review of any findings or recommendations resulting from the surety assessment and in making determinations for how to move forward.

Best Regards,

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

David Darnell
Co-Chair, NAESB Critical Infrastructure Committee

cc: Mr. Christopher Freitas, Office of Oil and Natural Gas, U.S. Department of Energy
Ms. Rae McQuade, President and COO, North American Energy Standards Board
Mr. Jonathan Booe, Vice President and CAO, North American Energy Standards Board