Via posting

November 14, 2019

**TO:** NAESB Board Strategy Committee

**FROM:** Michael Desselle, NAESB Chairman of the Board of Directors, Chair of the NAESB Digital Committee

**RE:** Sandia Surety Assessment Recommendations/Considerations

Dear Committee Members,

As you know, in April 2017, NAESB announced that the Department of Energy had generously offered to provide a surety assessment of the NAESB Business Practice Standards to be performed by Sandia National Laboratories (Sandia). Sandia previously performed two surety assessments on the NAESB Business Practice Standards in 2006 and 2000 and, in both cases, modifications were made to the standards as a result of the laboratories’ recommendations. Over the course of two years, NAESB subject matter experts, NAESB staff and the NAESB Critical Infrastructure Committee worked closely with Sandia staff to provide information on specific standards identified by the assessment team concerning how the identified standards are utilized by the market and to provide feedback on the five draft iterations of the surety assessment reports provided by Sandia.

On July 22, 2019, SNL provided NAESB with four final 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. In total, across the four reports, Sandia National Laboratories made twelve recommendations to mitigate security issues and identified twenty-two additional findings or considerations. In each of the reports, findings or considerations were put forward that did not directly impact the existing NAESB standards or describe a current activity or responsibility of NAESB as an organization. These items have been reviewed by the NAESB Critical Infrastructure Committee and the NAESB Digital Committee and a recommendation has been made that the Board Strategy Committee evaluate these 11 items and propose any new activities or responsibilities that the NAESB Board of Directors should consider in response. A description of the 11 items is included as an attachment to this work paper.

Additionally, through discussions with the Department of Energy and Sandia, an informal recommendation was made for NAESB, working with the FERC and the Department of Energy, to consider a new model for the implementation of its cybersecurity standards. Specifically, it was noted that the process of developing and/or modifying cybersecurity standards through NAESB and submitting those standards to FERC for consideration as part of a possible rulemaking prior to implementation by the industry requires a minimum amount of time that may be untenable to ensure base level protections are being employed by all parties to transactions within the industry. In response to this request and to support market needs, recognizing that immediate responses are typically necessary to adequately mitigate cyber threats, this committee will review the NAESB process and procedures and recommend any necessary modifications for consideration by the Board of Directors.

With Best Regards,

|  |
| --- |
| MDSignature |
| Michael Desselle  NAESB Chairman of the Board of Directors  Chair of the NAESB Digital Committee |

**Assessment Report of the NAESB Public Key Infrastructure Program**

*Additional Findings or Considerations*

As part of the Assessment Report of the NAESB Public Key Infrastructure Program, the Critical Infrastructure Committee identified one area as part of the additional findings and considerations made by Sandia National Laboratories that would need a determination by the Board of Directors on how to proceed. This finding or consideration was made by Sandia National Laboratories as part of Section 4 Metrics of Importance.

| **Issue** | **Report Section (Page Number)** | **Sandia Finding or Consideration** | **Standard Consideration (if applicable)** | **Assignment (if applicable)** |
| --- | --- | --- | --- | --- |
| 3. | PKI Report Section 4 – Metrics of Importance (Page 9) | Metrics should be collected and analyzed to measure how the implementation of the PKI program increases the security and reliability of electronic data exchanges between trading partners. The following are some examples of metrics related to the PKI program that could be collected for NAESB and industry partners:   * Measure overall ACA activity including the number of new or renewed certificates issued, number of rejected requests, number of certificate revocations, and number of security anomalies[[1]](#footnote-1) * Measure the best, median, average, and worst time it takes for an organization to detect, report, notify trading partners and the ACA about a compromised certificate * Measure the best, median, average, and worst time for an updated revocation list to be issued for a compromised certificate * Measure an organization’s level of compliance with updated revocation lists (i.e. – Are they checking for an updated revocation list with each transaction, or are they using some other time period) * Measure the number of certificate compromises per organization * Time for an ACA to issue a new certificate if the previous certificate was compromised   For the ACA metrics, NAESB could incorporate these statistics into required reporting during the annual ACA recertification process. For other organizations, these statistics could be self-reported – either to NAESB or maintained on a statistics webpage. If desired, NAESB could collect and tabulate the totals annually and then share the information with participating organizations. If necessary, data could be anonymized while still allowing organizations to rate their own performance against the industry norms.  This data could then be used in life-cycle decisions, trading partner selection, or determining if NAESB standards need to be upgraded or revised. | This is not currently a requirement of the NAESB standards nor is this a function currently provided by NAESB  Industry may want to consider if there is a benefit to individual entities tracking information identified by the metrics.  This issue should be discussed by the NAESB Board of Directors for a determination on how to proceed. | N/A |

**Assessment Report of the NAESB OASIS Standards**

*Security Issues*

As part of the Assessment Report of the NAESB OASIS Standards, the Critical Infrastructure Committee identified one recommendation made by Sandia National Laboratories addressing a security issue that would need a determination by the Board of Directors on how to proceed. This recommendation was made as part of a series of recommendations to address Section 6.1 of the report, which Sandia National Laboratories indicated addresses “vulnerabilities that could provide an opportunity to an attacker to conduct malicious activities that would affect the availability or security of OASIS Nodes, compromise the sensitive information stored on those nodes, or interrupt business transactions conducted using OASIS.”

| **Issue** | **Report Section (Page Number)** | **Sandia Recommendation** | **Recommended Standards Development Activity** | **Recommended Assignment** |
| --- | --- | --- | --- | --- |
|  | OASIS Report Section 6.1.1 – Significant Amounts of Sensitive Information are Posted on OASIS (Pages 11 – 12) | Level: Low  Continue to leverage the NAESB OASIS Subcommittee to ensure there is a balance between protecting sensitive information and meeting industry needs. In addition, the assessment team recommends that NAESB work with their partners and FERC to determine if more stringent security testing – similar to that used for ACAs – is desirable for OASIS Node operators to ensure the nodes are secure from cyber attacks. | This is not an area NAESB currently addresses.  Board action or direction may be needed regarding the exploration of the development of security testing. This issue should be discussed by the NAESB Board of Directors for a determination on how to proceed. | N/A |

*Additional Findings or Considerations*

As part of the Assessment Report of the NAESB OASIS Standards, the Critical Infrastructure Committee identified one area as part of the additional findings and considerations made by Sandia National Laboratories that would need a determination by the Board of Directors on how to proceed. This finding or consideration was made by Sandia National Laboratories as part of Section 4 Metrics of Importance.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Issue** | **Report Section (Page Number)** | **Sandia Recommendation** | **Recommended Standards Development Activity** | **Recommended Assignment** |
| 6. | OASIS Report Section 4 – Metrics of Importance (Pages 9 – 10) | Metrics should be collected and analyzed to measure how the implementation of the OASIS Standards increases the usability, security and reliability of conducting transactions through OASIS Nodes.  The following are some examples of metrics that could be collected for NAESB and industry partners to review and analyze:   * Measure the total number of OASIS users, and the number of OASIS observers * Collect the type and version of web browsers used to access OASIS * Enumerate the encryption methods used by the browsers to access OASIS information and note any requests for downgrading encryption to any type that does not meet security requirements (including encryption type “NONE”) * Collect information on what pages and documents are accessed by various accounts * Count the number of users that have an individual account, and the number of users that use a shared “entity” account * Measure the number of daily transactions between business partners, and the number of transactions that fail or have errors that need to be corrected * Measure the overall dollar amount of transactions completed each month * Measure the best, median, average, and worst time for a transaction to be completed * Using IP Geolocation, identify the number of logins that are completed from an unexpected geographic region * Log the time of a user login, the average time they remain logged in, and the number of actions (pages/documents accessed, etc.) during the session   The various OASIS Nodes could maintain this information and submit the information to NAESB monthly to allow this information to be tabulated and shared with participating organizations. If necessary, data could be anonymized while still allowing organizations to rate their own performance against the industry norms.  This data could then be used in life-cycle decisions, identifying security anomalies, identifying poor security practices at an organization, or determining if NAESB standards need to be upgraded or revised to address any issues discovered. | This is not currently a requirement of the NAESB standards nor is this a function currently provided by NAESB  Industry may want to consider if there is a benefit to individual entities tracking information identified by the metrics.  This issue should be discussed by the NAESB Board of Directors for a determination on how to proceed. | N/A |

**Assessment Report of the NAESB Business Operations Practices and Standards**

*Additional Findings and Considerations*

As part of the Assessment Report of the NAESB Business Operations Practices and Standards, the Critical Infrastructure Committee identified two areas as part of the additional findings and considerations made by Sandia National Laboratories that would need a determination by the Board of Directors on how to proceed. This finding or consideration was made by Sandia National Laboratories as part of Section 4 Metrics of Importance and Section 6.2.2 Separation of Business and Control Computer Networks. As indicated by Sandia National Laboratories, these two sections address metrics and “areas the assessment team identified as practices or requirements that prevented or increased the difficulty of a successful attack or exploitation by an adversary.”

| **Issue** | **Report Section (Page Number)** | **Sandia Finding or Consideration** | **Standard Considerations (if applicable)** | **Assignment (if applicable)** |
| --- | --- | --- | --- | --- |
| 6. | Business Operations Practices and Standards Report Section 4 – Metrics of Importance (Pages 8 – 9) | Metrics should be collected and analyzed to measure how the implementation of the Business Operations Practices and Standards increases the reliability and security of electronic data exchanged between trading partners. The following are some examples of metrics that could be collected for NAESB and industry partners to review and analyze:   * Measure the number of daily transactions between business partners, and the number of transactions that fail or have errors that need to be corrected * Measure the best, median, average, and worst time for a transaction to be completed * Count the number of organizations that have established continuity of operations planning (COOP), and the number of organizations that exercise their COOP each year * Count the number of organizations that maintain alternate and 24/7 contact information for trading partners, and the number that have this information stored offline (in case of a ransomware attack) * Count the number of times alternate methods were used for transactions (ex. phone or fax) during normal operations; and during a system outage, failure, or other issue   These metrics could be self-reported – either to NAESB or maintained by each organization on a statistics webpage that can be accessed by their trading partners. If desired, NAESB could collect and tabulate the totals on a monthly basis, and then share the information with participating organizations. If necessary, data could be anonymized while still allowing organizations to rate their own performance against the industry norms.  This data could then be used in life-cycle decisions, trading partner selection, analysis of COOP and disaster recovery plans, and determining if NAESB standards need to be upgraded or revised. | This is not currently a requirement of the NAESB standards nor is this a function currently provided by NAESB  Industry may want to consider if there is a benefit to individual entities tracking information identified by the metrics.  This issue should be discussed by the NAESB Board of Directors for a determination on how to proceed. | N/A |
| 8. | Business Operations Practices and Standards Report Section 6.1.5 – Separation of Business and Control Computer Networks (Page 12 – 13)  (Table of Contents Section 6.2.2 Separation of Business and Control Computer Networks) | Some commonly suggested security solutions are to isolate the SCADA and PCN systems from the Internet and corporate enterprise network (EN) through the use of firewalls, which can be complex devices to design and deploy correctly, data diode separation which allows network data to flow in one direction allowing for monitoring of control systems but not allowing control signals to traverse from the business side network to the control network, virtual private network implementation which restricts access to designated portions of the network, internet protocol security (IP sec) which is a protocol implementation designed to require encryption between two devices and requires a shared public key.  This Centre for the Protection of National Infrastructure (CPNI) Good Practice document addresses the need for guidance in creating such firewalls. There are a significant number of different solutions used by the industry and the security effectiveness of these can vary widely. In general, architectures that allow the establishment of a Demilitarized Zone (DMZ) between the enterprise network and SCADA/PCN network will provide the most effective security solution. Realize this part of defense-in-depth strategy. Here is more complete treatment [[2]](#footnote-2)  Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, Industrial Control Systems Cyber Emergency Response Team, September 2016. | This is not currently a requirement of the NAESB standards nor is this a function currently provided by NAESB.  This issue should be discussed by the NAESB Board of Directors for a determination on how to proceed. | N/A |

**Addendum Report: Threat-based Examination of NAESB Standards and Business Operations**

As part of the Addendum Report: Threat-based Examination of NAESB Standards and Business Operations, the Critical Infrastructure Committee identified four areas as part of the additional findings and considerations made by Sandia National Laboratories that would need a determination by the Board of Directors on how to proceed. This finding or consideration was made by Sandia National Laboratories as part of Section 2.3.1 EDI Cyber Attack and Section 3.1 Trends in Operation. These two sections address the April 2018 EDI cyber attack and future trends in operations/technical areas that are expected to be adopted in the future.

| **Issue** | **Report Section (Page Number)** | **Sandia Finding or Consideration** | **Standards Considerations (if applicable)** | **Assignment (if applicable)** |
| --- | --- | --- | --- | --- |
| 1. | Addendum Report Section 2.3.1 – EDI Cyber Attack (Pages 21 – 23) | To better understand the impact this kind of outage has on business operations and operating costs, the team has identified several metrics that could be used to help quantify the impact of these kinds of events:   * Measure the number of daily transactions during normal operations and the number of daily transactions when using COOP procedures. * Measure the number of hours worked by staff during normal operations and during COOP procedures. This should also include any time spent on recovering local systems or testing to ensure functionality of remote systems has been restored. * Measure any additional expenses incurred due to utilizing COOP procedures. For example, if food must be provided due to staff working additional hours; or expenses due to overtime wages. * Measure the number of errors made in transactions during normal operations, and the number of errors made when using COOP procedures. * Measure the time the outage began, to the time full service is restored. * Measure the time and expense to perform a forensic analysis of affected systems to determine the root cause of the attack or failure. * Count the number of organizations affected by the outage.   Following a major outage, these metrics could be reported to NAESB to tabulate the total cost and impact of the event. This data could then be used in life-cycle decisions, vendor selection, analysis of continuity of operations/disaster recovery planning, and to determine if NAESB standards need to be upgraded or revised. | This is not currently a requirement of the NAESB standards nor is this a function currently provided by NAESB  Industry may want to consider if there is a benefit to individual entities tracking information identified by the metrics.  This issue should be discussed by the NAESB Board of Directors for a determination on how to proceed. | N/A |
| 2. | Addendum Report Section 2.3.1 – EDI Cyber Attack (Pages 21 – 23) | The assessment team recommends that NAESB work through their existing relationships with TSA and NERC to develop more-detailed guidance on cyber security plans (including incident response procedures). An important recommendation is to ensure that NAESB members receive relevant cyber attack incident reporting. In addition to NAESB partner organizations above there exists a large resource of existing federal organizations with capability and responsibility to help in cyber security attacks against critical infrastructure. *Appendix C describes those organizations, their roles and responsibilities, capabilities and contact mechanisms*.  These recommendations are not intended to be used as a guide for compliance, or to replace current reporting that is required by the FERC or other federal or state regulatory agencies as this is outside the scope of the assessment. | This is not currently a requirement of the NAESB standards nor is this a function currently provided by NAESB.  Coordination with other organizations is a function of the NAESB Board of Directors. This issue should be discussed by the NAESB Board of Directors for a determination on how to proceed. | N/A |
| 3. | Addendum Report Section 2.3.1 – EDI Cyber Attack (Pages 21 – 23) | Another part of the TSA/NERC engagement, would be to consider initiating development of incident report templates relevant to their stakeholders. Such a template, although likely voluntary, would ensure reporting is more complete and the standardization could include examples to help socialize the needs and improve relationships…  These reports can take the shape of a wizard driven reporting mechanism that populates a database such as the US CERT[[3]](#footnote-3), DHS[[4]](#footnote-4) and DOE[[5]](#footnote-5) incident report portals or develop your own document using guidance from NIST Computer Security Incident Handling Guide.  These recommendations are not intended to be used as a guide for compliance, or to replace current reporting that is required by the FERC or other federal or state regulatory agencies as this is outside the scope of the assessment. | This is not currently a requirement of the NAESB standards nor is this a function currently provided by NAESB.  Coordination with other organizations is a function of the NAESB Board of Directors. This issue should be discussed by the NAESB Board of Directors for a determination on how to proceed. | N/A |
| 6. | Addendum Report Section 3.1 – Trends in Operation (Pages 26 – 27) | As technology is integrated into the control systems, it is important to ensure that abnormal events can be detected and that abnormal conditions do not prevent operations from being conducted or, after an outage, from being restored. To ensure that problems can be detected, the assessment team recommends that existing metering be used to verify information being provided by the control systems and, in the event that the computer system and the metering system disagree, that response personnel can be deployed to investigate in a timely manner. However, to ensure that response personnel are able to manually restore proper functioning, the assessment team notes it is imperative that the responders have a method to disconnect the equipment from the control network and conduct manual operations until normal operations can be restored. | This is not currently a requirement of the NAESB standards nor is this a function currently provided by NAESB.  This issue should be discussed by the NAESB Board of Directors for a determination on how to proceed. | N/A |

1. A security anomaly would be anything unusual enough, or serious enough, to be noted. For example, a known criminal organization attempting to obtain a certificate. [↑](#footnote-ref-1)
2. (<https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf>) [↑](#footnote-ref-2)
3. US-CERT Incident Reporting System, <https://www.us-cert.gov/forms/report> [↑](#footnote-ref-3)
4. Report Cyber Incidents, <https://www.dhs.gov/how-do-i/report-cyber-incidents> [↑](#footnote-ref-4)
5. DOE - JC3 Incident Reporting, <https://tickets.ijc3.doe.gov> [↑](#footnote-ref-5)