**TO:** All Interested Parties

**FROM:** Board CIC Chair and Vice Chair

**RE: Proposed Surety Assessment Standard Development Activities and Assignments Chairs’ Work Paper – NAESB PKI Program Report**

Proposed Surety Assessment Standard Development Activities and Assignments – NAESB PKI Program Report – DRAFT

On July 22, 2019, Sandia National Laboratories provided NAESB with the final reports on the surety assessment: (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 anticipation of these reports being delivered, NAESB included on its 2019 Annual Plans a review of the final reports and the development and/or modifications of NAESB Business Practice Standards as needed to address recommendations from Sandia National Laboratories. The Department of Energy has requested that, where possible, NAESB expediate any resulting standard development. To assist in these efforts, the Critical Infrastructure Committee has committed to reviewing the final reports to provide context to any recommendations containing actionable items for standards development.

**Security Issues**

The first section of this work paper identifies items identified as part of Section 6.1 Security Issues of the Assessment Report of the NAESB Public Key Infrastructure Program and contains the specific standard development efforts identified by the Board Critical Infrastructure Committee that NAESB should consider in response. As indicated by Sandia National Laboratories, Section 6.1 addresses “vulnerabilities that could provide an opportunity to an attacker wishing to conduct malicious activities that would affect the establishment or maintenance of an ACA and the issuance and revocation of certificates.” As part of Section 6.1, Sandia National Laboratories has identified two areas of vulnerability: Section 6.1.1 Discrepancy between NAESB Standards and Certification Practice Statements and Section 6.1.2 Possible Incomplete Enforcement of NAESB Standards Assurance Levels. Within these two subsections, Sandia National Laboratories has provided two recommendations to address the identified vulnerabilities.

Sandia National Laboratories assigned a level of severity for each vulnerability: (1) High – represents a systemic weakness which could allow an adversary to directly and/or covertly conduct malicious activity; (2) Moderate – represents a weakness which could allow an adversary to conduct malicious activity and cause considerable degradation of operations; or (3) Low – represents a weakness which could allow an adversary to conduct malicious activity and cause targeted or limited impact on the mission.

The table below captures the two recommendations identified within Section 6.1 Security Issues and the corresponding standard development activities to address these recommendations.

| **Issue** | **Report Section (Page Number)** | **Sandia Recommendation** | **Recommended Standards Development Activity** | **Recommended Assignment** |
| --- | --- | --- | --- | --- |
|  | PKI Report Section 6.1.1 – Discrepancy between NAESB Standards and Certification Practice Statements (Pages 10 – 11) | Level: Low  The ACAs should include verbiage in the CPS that indicates a mismatch between the CPS and NAESB standard will default to the NAESB standard. Alternatively, the CPS could be updated to reference the appropriate NAESB standard(s) instead of including the language directly in the CPS. | Subcommittee should consider if the Accreditation Requirements for Authorized Certification Authorities should be modified to include a requirement that all Certification Practice Statements include a statement that in instances of a conflict between language, the NAESB Standards will have precedence. | WEQ Cybersecurity Subcommittee |
|  | PKI Report Section 6.1.2 – Possible Incomplete Enforcement of NAESB Standards Assurance Levels (Page 11) | Level: Low  Investigate if “High” assurance level certificates have been issued and review if there needs to be changes to the retention period in either the NAESB standard, or in the GlobalSign CPS. (Note: Section 4.4 Records Retention Policy of the OATI CPS indicates records will be retained for “time periods required by applicable standards”.) | Subcommittee should review the need to maintain a “High” assurance level and review all retention periods associated with each assurance level to determine if the requirements are still meeting industry needs and best practices. | WEQ Cybersecurity Subcommittee |

**Additional Findings and Considerations**

This section of the work paper identifies additional practices or recommendations identified by Sandia National Laboratories as part of Section 4 Metrics of Importance and Section 6.3 Review of X.509 Security of the Assessment Report of the NAESB Public Key Infrastructure Program and the related standard development activities identified by the Board Critical Infrastructure Committee that NAESB may want to consider in response. As indicated by Sandia National Laboratories, these sections of the report specifically addresses metrics and “security of X.509 certificates.” In total, there are three findings or considerations from Sandia National Laboratories.

The table below captures the three findings and the related standard considerations to potentially incorporate the identified concept into the standards, as applicable.

| **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. | N/A |
| 4. | PKI Report Section 6.3 – Review of X.509 Security (Page 12) | The assessment team recommends NAESB review the industry sources such as NIST NVD, ICS-CERT, US-CERT, SANS common weakness enumeration as part of their annual assessment and consider adding verbiage for organizations that rely on X.509 certificates review their systems and software to determine if they are utilizing technologies that are affected by these vulnerabilities (or any others) and update their systems and software to a version that is not affected.  Additionally, specific details on individual CVEs can be found in [NIST’s NVD](https://nvd.nist.gov/) along with “References to Advisories, Solutions, and Tools” for each CVE. | As part of a recurring WEQ Annual Plan Item, the WEQ Cybersecurity performs an annual assessment on the WEQ-012 PKI Standards and the Accreditation Requirements for Authorized Certification Authorities | WEQ Cybersecurity Subcommittee |
| 5. | PKI Report Section 6.3 – Review of X.509 Security (Page 12) | As included in the Wholesale Gas Electronic Delivery Mechanism Related Standards and incorporated by FERC in 18 CFR 284.12, updating to the latest versions of available protocols as soon as practicable and not to exceed 9 months is a general best practice that organizations within the wholesale electric quadrant and users of X.509 certificates should also follow. NAESB may want to consider the development of similar wholesale electric business practice standards. | The WGQ EDM Manual Appendices B and D state entities should seek to utilize the latest generally available version of a software/protocol within 9 months of such version becoming available  Subcommittee should consider the applicability/benefit or such a requirement for WEQ Standards | WEQ Cybersecurity Subcommittee |

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)