**TO:** All Interested Parties

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

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

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

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. The table below identifies the explicit findings and other recommendations in the Assessment Report of the NAESB PKI Program and the corresponding standard development activities to address the recommendations from Sandia National Laboratories.

| **Issue** | **Report Section (Page Number)** | **Sandia Finding/Recommendation** | **Recommended Standards Development Activity** | **Recommended Assignment** |
| --- | --- | --- | --- | --- |
|  | PKI Report Section 4 – Metrics of Importance (Page 9) | Level: N/AMetrics 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. |  |  |
|  | PKI Report Section 6.1.1 – Discrepancy between NAESB Standards and Certification Practice Statements (Pages 10 – 11)  | Level: LowThe 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. |  |  |
|  | PKI Report Section 6.1.2 – Possible Incomplete Enforcement of NAESB Standards Assurance Levels (Page 11) | Level: LowInvestigate 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”.) |  |  |
|  | PKI Report Section 6.3 – Review of X.509 Security (Page 12) | Level: N/AThe 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. |  |  |
|  | PKI Report Section 6.3 – Review of X.509 Security (Page 12) | Level: N/AAs 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. |  |  |

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)