**TO:** All Interested Parties

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

**RE: Proposed Surety Assessment Standard Development Activities and Assignments Chairs’ Work Paper – NAESB OASIS Standards**

Proposed Surety Assessment Standard Development Activities and Assignments – NAESB OASIS Standards – 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 addresses items identified as part of Section 6.1 Security Issues of the Assessment Report of the NAESB OASIS Standards 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 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.” As part of Section 6.1, Sandia National Laboratories has identified two areas of vulnerability: Section 6.1.1 Significant Amounts of Sensitive Information Are Posted on OASIS and Section 6.1.2 Implementation Details for OASIS Nodes Not Specified. Within these two subsections, Sandia National Laboratories has provided five 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 five 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** |
| --- | --- | --- | --- | --- |
|  | OASIS Report Section 6.1.1 – Significant Amounts of Sensitive Information are Posted on OASIS (Pages 11 – 12) | Level: LowContinue 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 | N/A |
|  | OASIS Report Section 6.1.1 – Significant Amounts of Sensitive Information are Posted on OASIS (Pages 11 – 12)  | Level: LowThe assessment team recommends review of NIST SP 800-63-3 section 4.1.1 and review for implementation new approved technologies supporting authentication methods. | There is not a Section 4.1.1 in NIST SP 800-63-3, but [NIST SP 800-63-3B Authentication and Lifecycle Management](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf) does have a Section 4.1.1 Permitted Authenticator Types that identify nine different authenticator types and Section 5 Authenticator and Verifier Requirements contain detailed requirements for each type of authenticator. The Addendum Report Section 2.3.2 states that the authentication method in the OASIS Standards (WEQ-002-5.1.1) is considered adequate and consistent with current business practicesReview the current OASIS requirements for authentication, especially regarding passwords, against the recommended best practices in NIST SP 800-63-3B and revise standards as needed. | Jointly between WEQ OASIS Subcommittee and WEQ Cybersecurity Subcommittee |
|  | OASIS Report Section 6.1.1 – Significant Amounts of Sensitive Information are Posted on OASIS  | Level: LowAdditionally, the assessment team recommends that WEQ-002 be reviewed with consideration to incorporate NIST 800-52 details for TLS version and associated configurations which currently requires version 1.2 and support for version 1.3 by January 1, 2021. Specific configurations for TLS servers and TLS versions are detailed in section 4 of NIST 800-52 and the specific server implementation is dependent on the TLS version and implementation strategy. SSL protocol is disallowed for both government and business – facing applications and as such, the assessment team recommends disallowing support for SSL version protocols and removal of references to SSL versions and exclusively callout TLS version 1.2 configured with validated FIPS-140-2 modules[[1]](#footnote-1) | The subcommittees should review TLS/SSL references and update the standard(s) accordingly as recommended | Jointly between WEQ OASIS Subcommittee and WEQ Cybersecurity Subcommittee |
|  | OASIS Report Section 6.1.1 – Significant Amounts of Sensitive Information are Posted on OASIS  | Level: LowThe team recommends that the OASIS Subcommittee consider the sensitivity of historical information and determine what information can be removed on a quarterly basis; | Subcommittee should review all OASIS standards that specify data retention. | WEQ OASIS Subcommittee |
|  | OASIS Report Section 6.1.2 – Implementation Details for OASIS Nodes Unspecified (Pages 12 – 14)  | Level: LowTo mitigate this issue, the assessment team recommends that all OASIS nodes follow industry best practices to secure their systems. This would include, but is not limited to: * Ensuring web applications are secure against common vulnerabilities such as the OWASP Top 10[[2]](#footnote-2) OWASP addresses common vectors for attack, and methods for prevention for each identified security risk.
* Encrypting all communications (as allowable) using an encryption module that is validated against FIPS 140-2[[3]](#footnote-3),[[4]](#footnote-4) . The assessment team recommends removal of HTTP communication for status notifications and utilizing either HTTPS solutions or utilize encrypted email notification. In section WEQ-002-5.1 appears to require encrypted communication but in WEQ-002-4.2 allowances are made for HTTP notifications. NIST SP 800-131A REV 2 provides guidance for acceptable encryption (AES 128 bit or better), random bit generation, hash functions and message authentication codes.
* Utilizing the latest versions of all critical standards (such as TLS) to ensure all possible vulnerabilities are addressed
* Verifying and validating all external inputs
* Conducting business continuity and disaster recovery exercises on an annual basis
* Applying patches and updates in a timely manner; ideally no longer than 7 days after the patch or update becomes available (if practical). It is imperative that implementation details, system configurations, and software dependencies be considered prior to applying updates as some updates can have a detrimental impact on functionality. Any of these items that have an impact on the update process must be tracked and communicated to dependent parties.
 | Subcommittees should consider additional standard(s) ensuring web applications are secure against common vulnerabilities such as the OWASP Top 10Subcommittees should review encryption of OASIS data and references to HTTP/HTTPS as recommended and modify standards as neededSubcommittees should consider standard(s) to require business continuity and disaster recover exercises on an annual basis as recommendedSubcommittees should consider standard(s) to require applying patches and updates in a timely manner; ideally no longer than 7 days after the patch or update becomes available as recommended | Jointly between WEQ OASIS Subcommittee and WEQ Cybersecurity Subcommittee |

**Additional Findings and Considerations**

This section of the work paper identifies additional findings and considerations identified by Sandia National Laboratories as part of 4 Metrics of Importance of the Assessment Report of the NAESB OASIS Standards 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, this section of the report specifically addresses metrics. There is one finding from Sandia National Laboratories within this section.

The table below captures the finding and 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)** |
| --- | --- | --- | --- | --- |
| 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 NAESBIndustry may want to consider if there is a benefit to individual entities tracking information identified by the metrics.May want to discuss at Board of Directors level | N/A |

1. NIST 800-52 section 3.1 Protocol Version Support <https://csrc.nist.gov/CSRC/media/Publications/sp/800-52/rev-2/draft/documents/sp800-52r2-draft2.pdf> [↑](#footnote-ref-1)
2. <https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf> [↑](#footnote-ref-2)
3. FIPS 140-2: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf> [↑](#footnote-ref-3)
4. Validated encryption modules: <https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules> [↑](#footnote-ref-4)