WEQ Cybersecurity Subcommittee Assignments

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.

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

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 assigned to the WEQ Cybersecurity Subcommittee

| **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  Requirement may already be addressed by recent changes to ACA Specification and requirements as part of certification program to use most recent version of specification. Certificate authorities also have to adhere to other industry standards. |
|  | 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  The subcommittee will discuss the need to maintain “High” assurance level. |

**Assessment Report of the NAESB OASIS Standards**

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 assigned jointly to the WEQ Cybersecurity Subcommittee and WEQ OASIS Subcommittee.

| **Issue** | **Report Section (Page Number)** | **Sandia Recommendation** | **Recommended Standards Development Activity** | **Recommended Assignment** |
| --- | --- | --- | --- | --- |
| 2. | OASIS Report Section 6.1.1 – Significant Amounts of Sensitive Information are Posted on OASIS (Pages 11 – 12) | Level: Low  The 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 practices  Review 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: Low  Additionally, 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 |
| 5. | OASIS Report Section 6.1.2 – Implementation Details for OASIS Nodes Unspecified (Pages 12 – 14) | Level: Low  To 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 10  Subcommittees should review encryption of OASIS data and references to HTTP/HTTPS as recommended and modify standards as needed  Subcommittees should consider standard(s) to require business continuity and disaster recover exercises on an annual basis as recommended  Subcommittees 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 |

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

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, assigned to the WEQ Cybersecurity Subcommittee.

| **Issue** | **Report Section (Page Number)** | **Sandia Finding or Consideration** | **Standard Consideration (if applicable)** | **Assignment (if applicable)** |
| --- | --- | --- | --- | --- |
| 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  NAESB staff maintains a list of activities and documents for the WEQ Cybersecurity Subcommittee to review as part of the recurring annual plan items and can add this to the list.  The WEQ Cybersecurity Subcommittee already performs an annual assessment and can include review of the NIST NVD as part of this review. | WEQ Cybersecurity Subcommittee  This is included as part of the recurring annual plan items, and the subcommittee will incorporate these specific documents as part of its annual review as necessary. |
| 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  The ACA Specification requires the ACAs use the most recent versions of protocols.  Subcommittee will discuss need for WEQ standard applicable to end entities or within the WEQ OASIS Standards. |

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

Additional Findings and Considerations

This section of this work paper identifies additional findings and considerations identified by Sandia National Laboratories as part of Section 4 Metrics of Importance and Section 6.2 Strengths of the NAESB Business Operations Practices and Standards of the Assessment Report of the NAESB Business Operations Practices and 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, these two sections of the report specifically 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. Within Section 4 Metrics, there is one area of consideration. As part of Section 6.2 Strengths of the NAESB Business Operations Practices and Standards, there are three areas of consideration: Section 6.2.1 Use of Human control and Review of Operations, Section 6.2.2 Separation of Business and Control Computer Networks, and Section 6.2.3 Gas and Electric Industry Interactions. In total, there are eight findings or considerations from Sandia National Laboratories.

The table below captures the eight findings and the related standard considerations to potentially incorporate the identified concept into the standards, as applicable, assigned to the WEQ Cybersecurity Subcommittee.

| **Issue** | **Report Section (Page Number)** | **Sandia Finding or Consideration** | **Standard Considerations (if applicable)** | **Assignment (if applicable)** |
| --- | --- | --- | --- | --- |
| 7. | Business Operations Practices and Standards Report Section 6.1.4 – Use of Human Control and Review in Operations (Page 12)  (Table of Contents Section 6.2.1 Use of Human Control and Review in Operations) | With the current trend towards more automation and computer control, this strength should be considered when replacing human operators with autonomous systems. Many tools exist to help automate both security of network systems and can provide additional support for monitoring network traffic and operations through technologies such as Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), machine learning, user behavioral analysis, zero trust models or other technologies that may become available. These are implementation details that may optionally be reviewed for acceptable standards.[[5]](#footnote-5) This includes recommended guidelines for configuration and even logging, network traffic monitoring, and alerting systems. The assessment team also recommends that, at a minimum, humans retain monitoring capability and where possible provide manual continuity of operations in the event of abnormal behavior or failure conditions with the system. | Subcommittees should consider standard(s) to address recommended guidelines for configuration and logging, network traffic monitoring, and alerting systems as well standard(s) requiring manual continuity of operations in the event of abnormal behavior or failure conditions with the system. | WEQ Cybersecurity Subcommittee should investigate applicability to WEQ Business Practice Standards  This could have potential applicability to OASIS and e-Tagging but needs additional discussion. This discussion will likely need to include input from other subcommittees and WEQ EC. |
| 9. | Business Operations Practices and Standards Report – Section 6.1.6 Continued Use of Different Security Paradigms (Pages 13 – 15)  (Table of Contents Section 6.2.3 Gas and Electric Industry Interactions) | Both PGP and PKI provide adequate security provided they are properly configured and NIST - 131A encryption and decryptions denotes AES encryption and decryption as acceptable. NIST - 131A makes allowance for some legacy encryption and decryption algorithms, the assessment team recommends removal of legacy support and a minimum encryption strength of 128 bits. This is consistent with NAESB Internet Electronic Transport standards which requires 128-bit strength encryption. | Subcommittees should review the standards for legacy support references and remove as recommended. | WEQ Cybersecurity Subcommittee |
| 12. | Business Operations Practices and Standards Report – Section 6.1.6 Continued Use of Different Security Paradigms (Pages 13 – 15)  (Table of Contents Section 6.2.3 Gas and Electric Industry Interactions) | Key lengths must be updated to reflect current acceptable encryption strength[[6]](#footnote-6). Specifically, RSA keys must be no shorter than 2048 bits, while ECDSA keys must be no shorter than 224 bits. Hash algorithms should be from the SHA-2 or SHA-3 families. Acceptable AES key lengths range from 128, to 192, to 256. In general, implementors should use the largest feasible key length consistent with implementation of current business processes. In order to be in compliance with these stronger algorithms, any PGP command line clients should be at version 9 or greater as earlier versions did not support SHA-2 or SHA-3 family hashing algorithms or fully support AES[[7]](#footnote-7). | Review and revise as recommended the NAESB Accreditation Requirements for Certificate Authorities (Section 5.1.6 Key Sizes) currently specifies:   * 2048 bit RSA/DSA key length and 160 bit ECDSA key length * 4096 bit RSA/DSA key length and 256 bit ECDSA key length for certificates expiring after 12/31/2012 * 3072 bit RSA/DSA for certificates expiring after 12/31/2030 * SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512 has algorithms | WEQ Cybersecurity Subcommittee  The subcommittee will review this section, remove legacy items, and update to reflect most current industry guidelines and best practices. |
| 13. | Business Operations Practices and Standards Report – Section 6.1.6 Continued Use of Different Security Paradigms (Pages 13 – 15)  (Table of Contents Section 6.2.3 Gas and Electric Industry Interactions) | Finally, IET business process as currently implemented may be vulnerable to both replay[[8]](#footnote-8) and amplification[[9]](#footnote-9) attacks. Based on the assessment teams review of the transactional process these two attacks were immediately identified as attacks of concern…  Note that this attack is feasible even with payloads that are encrypted with foreign, untrusted keys, or with payloads that are filled with garbage bits. Two basic approaches exist to help eliminate this kind of amplification attack. The first strategy involves making error notification messages to be as small as possible and smaller than the original requests. This way, an attacker using this mechanism will not be able to amplify the volume of data sent to a target; rather, as the response message is smaller, the overall denial-of-service risk will be correspondingly lowered. The second strategy uses rate limiting to ensure that error messages are sent at a rate that is lower than expected message processing speeds. This way, even if the responses are larger than the adversary-submitted requests, they will not be sent to the target at a rate that would strain target computational resources. | The subcommittees should consider standard(s) to address mitigation of replay and amplification attacks as aligned with recommended strategies | WEQ Cybersecurity Subcommittee |

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

Additional Findings and Considerations

This work paper identifies the additional findings and considerations identified by Sandia National Laboratories in the Addendum Report: Threat-based Examination of NAESB Standards and Business Operations and the related standard development activities identified by the Board Critical Infrastructure Committee that NAESB may want to consider in response. As part of this report, Sandia National Laboratories identifies ten considerations across six different sections: Section 2.3.1 EDI Cyber Attack, Section 2.3.2 Ukrainian Power Grid Attack, Section 3.1 Trends in Operation, Section 3.2 Government and Industry Standards, Section 3.3 Emerging Technologies, and Section 3.4 Recommended Future Assessments.

The table below captures the ten findings and the related standard considerations to potentially incorporate the identified concept into the standards, as applicable, assigned to the WEQ Cybersecurity Subcommittee and jointly to the WEQ Cybersecurity Subcommittee and WEQ OASIS Subcommittee.

| **Issue** | **Report Section (Page Number)** | **Sandia Finding or Consideration** | **Standards Considerations (if applicable)** | **Assignment (if applicable)** |
| --- | --- | --- | --- | --- |
| 4. | Addendum Report Section 2.3.2 – Ukrainian Power Grid Attack (Pages 23 – 25) | Specific to NAESB standards, the WEQ-002-5.1.1 authentication method is considered adequate and consistent with current business practices. WGQ Standard 4.3.60 and WGQ Standard 10.3.16/RMQ Standard 7.3.16 both allow basic authentication; however, the assessment team recommends multi-factor (e.g. two-factor) authentication be required on *an individual basis*. Simply authenticating the nodes involved is not acceptable. | Review WEQ-012.1.9 (which allows for the issuance of digital certificates for (1) individual subscribers; (2) role; (3) device; and (4) application) and revise as needed based on recommendation | WEQ Cybersecurity Subcommittee |
| 9. | Addendum Report Section 3.4 – Recommended Future Assessments (Pages 29 – 30) | Since OASIS nodes are implemented independently, the team recommends conducting internal and external scans of the nodes on a quarterly basis, and a security assessment or penetration test. This testing would allow the identification of nodes that are using older/vulnerable versions of software, leak information about the system (ex. list software versions being used) or have vulnerable implementations of their web applications. Since each node can be unique in its software, environment, and supporting security systems, the assessment team recommends that the node owner perform these assessments on their own systems. According to best practices from SANS[[10]](#footnote-10): “Scans should be performed regularly on all software, services, or platforms (SPPs) that are available external to the organization. At a minimum, scans should be performed monthly.” | Subcommittees should review the recommendation and consider standard(s) recommending best practices or requiring internal/external scans of nodes and a security assessment/penetration test as recommended | Jointly between WEQ Cybersecurity Subcommittee and WEQ OASIS Subcommittee |

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)
5. NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS) <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf> [↑](#footnote-ref-5)
6. Barker, E. and Roginsky, A. NIST 800-131A: *Transitioning the Use of Cryptographic Algorithms and Key Lengths*. National Institute of Standards and Technology, 2019. [↑](#footnote-ref-6)
7. Symantec Corporation. *PGP Command Line 9.0 User’s Guide*. Symantec, 2006. [↑](#footnote-ref-7)
8. *Replay Attacks*, retrieved on June 10, 2019, from <https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/replay-attacks> [↑](#footnote-ref-8)
9. *DNS Amplification Attacks*, retrieved on June 10, 2019, from <https://www.us-cert.gov/ncas/alerts/TA13-088A> [↑](#footnote-ref-9)
10. <https://www.sans.org/security-resources/policies/application-security/pdf/web-application-security-policy> [↑](#footnote-ref-10)