**1. RECOMMENDED ACTION: EFFECT OF EC VOTE TO ACCEPT RECOMMENDED ACTION:**

|  |  |  |  |
| --- | --- | --- | --- |
| x | Accept as requested | x | Change to Existing Practice |
|  | Accept as modified below |  | Status Quo |
|  | Decline |  |  |

**2. TYPE OF DEVELOPMENT/MAINTENANCE**

|  |  |
| --- | --- |
| **Per Request:** | **Per Recommendation:** |
|  | Initiation |  | Initiation |
| x | Modification |  x  | Modification |
|  | Interpretation |  | Interpretation |
|  | Withdrawal |  | Withdrawal |
|  |  |  |  |
|  | Principle |  | Principle |
|  | Definition |  | Definition |
|  | Business Practice Standard |  | Business Practice Standard |
| x | Document | x | Document |
|  | Data Element |  | Data Element |
|  | Code Value |  | Code Value |
|  | X12 Implementation Guide |  | X12 Implementation Guide |
|  | Business Process Documentation |  | Business Process Documentation |

**3. RECOMMENDATION**

**SUMMARY:**

This Recommendation incorporates changes made to the NAESB Accreditation Requirements for Authorized Certification Authorities (specification) document as recommended by the Board Critical Infrastructure Committee based on the findings reported by Sandia National Laboratories as part of their surety assessment. In addition, the Cyber Security Subcommittee updated references in the document to incorporate the most current versions of any referenced external documentation, best practices, or industry specifications.

An updated NAESB Accreditation Requirements for Authorized Certification Authorities (specification) document is attached to this recommendation and includes the changes referenced below.

**4. SUPPORTING DOCUMENTATION**

**a. Description of Request:**

The full text of the request of 2019 Annual Plan for the Wholesale Electric Quadrant (WEQ):

|  |  |
| --- | --- |
| **6.** | **Develop and/or modify the NAESB Business Practice Standards if needed to address any recommendations resulting from the surety assessment performed by Sandia National Laboratories** |
|  | a) | Review the surety assessment performed by Sandia National Laboratories and determine if standard changes are necessary. | 4th Q, 2019 | Cybersecurity Subcommittee / OASIS Subcommittee |
|  | b) | Develop and/or modify the NAESB Business Practice Standards as needed to address the Security Issues identified by Sandia National Laboratories  |  |  |
|  |  | i) | Develop and/or modify WEQ-012 and/or the NAESB Accreditation Requirements for Authorized Certification Authorities as needed to address Security Issues identified by Sandia National Laboratories | 4th Q, 2019 | Cybersecurity Subcommittee |
|  | c) | Develop and/or modify the NAESB Business Practice Standards as needed to address the Additional Findings and Considerations identified by Sandia National Laboratories |  |  |
|  |  | i) | Develop and/or modify WEQ-012, the NAESB Accreditation Requirements for Authorized Certification Authorities and/or other standards as needed to address Additional Findings and Considerations identified by Sandia National Laboratories | 4th Q, 2019 | Cybersecurity Subcommittee |
|  |  |  |  |  |

**b. Description of Recommendation:**

The recommendation incorporates the suggested modifications to the NAESB Accreditation Requirements for Authorized Certification Authorities document based on the results of the Sandia National Laboratories surety assessment as proposed by the NAESB Board Critical Infrastructure Protection Committee.

Specifically, the following changes were incorporated regarding the CSS issues identified by the Board Critical Infrastructure Protection Committee.

**Cyber Security Subcommittee Assignments**

**Security Issues in Section 6.1**

| **Issue** | **Report Section (Page Number)** | **Sandia Recommendation** | **Recommended Standards Development Activity** | **Recommendation Action** |
| --- | --- | --- | --- | --- |
|  | 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. | 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. | The ACA Requirements document (specification) already requires ACAs to use the most recent versions of other industry standards. CSS revised Section 1.1 of the specification to indicate the document contains the minimum requirements ACAs must meet, including the NAESB standards. These standards may be exceeded. |
|  | 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”.) | 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.  | CSS determined to leave in the “High” assurance level in the case it may be used in the future., at which point the retention period issue can be revisited.Furthermore Globalsign revised it CPS to address this advice regarding high assurance.  |

**Additional Findings and Consideration**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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. | This is included as part of the recurring annual plan items, and the CSS will incorporate these specific documents as necessary as part of its annual review. |
| 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 availableSubcommittee should consider the applicability/benefit or such a requirement for WEQ Standards | The ACA Specification already requires that ACAs use the most current versions of protocols.The subcommittee believes that no additional WEQ-012 standards are necessary, based on the current versioning requirements in the specification. |
| 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. | CSS changed the key lengths and encryption methods, in section 5.16 of the specification to reflect the most current industry guidelines and best practices.This change removes the legacy attributes.  |
| 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[[1]](#footnote-1). 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[[2]](#footnote-2). | 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
 | CSS changed the key lengths and encryption methods, in section 5.16 of the specification to reflect the most current industry guidelines and best practices.  |

**Joint Cyber Security Subcommittee / OASIS Subcommittee Assignments**

The issues listed below were addressed in the Joint OASIS / CSS Recommendation. Where CSS undertook changes to the ACA specification on it's own these are specifically noted.

| **Issue** | **Report Section (Page Number)** | **Sandia Recommendation** | **Recommended Standards Development Activity** | **Recommendation Action** |
| --- | --- | --- | --- | --- |
| 2. | 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. | Issue addressed in the joint OASIS/CSS Recommendation. |
|  | 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[[3]](#footnote-3) | The subcommittees should review TLS/SSL references and update the standard(s) accordingly as recommended | WEQ-002 aspect addressed in the joint OASIS/CSS Recommendation.CSS revised sections 5.1.1, 5.1.2, 5.1.6, 5.1.7, 5.2.1 and 5.2.7 in the specification to update to the latest version of the Federal Information Processing Standards Security Requirements for Cryptographic Models (FIPS 140-3).  |
| 5. | 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[[4]](#footnote-4) 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[[5]](#footnote-5),[[6]](#footnote-6) . 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 | OASIS Nodes, TLS and HTTPS aspects addressed in the joint OASIS/CSS Recommendation.CSS revised sections 5.1.1, 5.1.2, 5.1.6, 5.1.7, 5.2.1 and 5.2.7 in the specification to update to the latest version of the Federal Information Processing Standards Security Requirements for Cryptographic Models (FIPS 140-3).Remaining issues set aside for future consideration / undertaking. |
| 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[[7]](#footnote-7): “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 | Issue addressed in the joint OASIS/CSS Recommendation. |
|  |  |  |  |  |

The attached updated NAESB Accreditation Requirements for Authorized Certification Authorities (specification) document is incorporated herein as part of this recommendation.

**c. Business Purpose:**

To establish needed modifications to the NAESB Accreditation Requirements for Authorized Certification Authorities document based on the results of the Sandia National Laboratories surety assessment as proposed by the NAESB Board Critical Infrastructure Protection Committee.

**d. Commentary/Rationale of Subcommittee(s)/Task Force(s):**

Reference Meeting Minutes

* CSS 08/20/2019
* CSS 09/29/2019
* CSS 09/10/2019
* CSS 09/16/2019
* CSS/OASIS 10/03/2019
* CSS 10/10/2019
* CSS ??
1. 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-1)
2. Symantec Corporation. *PGP Command Line 9.0 User’s Guide*. Symantec, 2006. [↑](#footnote-ref-2)
3. 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-3)
4. <https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf> [↑](#footnote-ref-4)
5. FIPS 140-2: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf> [↑](#footnote-ref-5)
6. Validated encryption modules: <https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules> [↑](#footnote-ref-6)
7. <https://www.sans.org/security-resources/policies/application-security/pdf/web-application-security-policy> [↑](#footnote-ref-7)