**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 |
| X | Business Practice Standard | X | Business Practice Standard |
|  | Document |  | 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 to the RMQ Model Business Practices as recommended by the Board Critical Infrastructure Committee based on the findings reported by Sandia National Laboratories as part of the 2019 surety assessment.

The RMQ Information Requirements and Technical Electronic Implementation Subcommittee (IR/TEIS) held joint meetings with the Wholesale Gas Quadrant (WGQ) Electronic Delivery Mechanisms (EDM) Subcommittee to address 2019 RMQ Annual Plan Items 6.a and 6.b. This recommendation contains modifications to RXQ.5 Quadrant-Specific Electronic Delivery Mechanism (QEDM) Model Business Practices and RXQ.7 Internet Electronic Transport (IET) Model Business Practices.

.

**Recommended Standards:**

See Attachments:

Attachment 1: List of Proposed Standards and Documents Changes <https://www.naesb.org/member_login_check.asp?doc=retail_2019_api_6_rec_attach1.docx>.

Attachment 2: RXQ.5 Quadrant-Specific Electronic Delivery Mechanism Model Business Practices (Redlined): <https://www.naesb.org/member_login_check.asp?doc=retail_2019_api_6_rec_attach2.docx>.

Attachment 3: RXQ.7 Internet Electronic Transport Model Business Practices (Redlined):

<https://www.naesb.org/member_login_check.asp?doc=retail_2019_api_6_rec_attach3.docx>.

**4. SUPPORTING DOCUMENTATION**

1. **Description of Request:**

The full text of 2019 RMQ Annual Plan Items 6.a and 6.b:

|  |  |
| --- | --- |
| **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.Status: Started | 4th Q, 2019 | Joint RMQ IR/TEIS and WGQ EDM Subcommittee |
|  | b. | Develop and/or modify the NAESB Model Business Practices as needed to address Security Issues identified by Sandia National LaboratoriesStatus: Started | 4th Q, 2019 | Joint RMQ IR/TEIS and WGQ EDM Subcommittee |

**b. Description of Recommendation:**

The recommendation incorporates the suggested modifications to the RXQ.5 QEDM and RXQ.7 IET Model Business Practices based on the results of the Sandia National Laboratories surety assessment as proposed by the NAESB Board Critical Infrastructure Committee.

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

| **Issue** | **Report Section (Page Number)** | **Sandia Recommendation** | **Recommended Standards Development Activity** | **Recommendation Action** |
| --- | --- | --- | --- | --- |
| One | Business Operations Practices and Standards Report Section 6.1.1 – NAESB Standards Refer to Vulnerable Versions of Communication Protocols (Page 10 – 11) | Level: HighIn addition, to ensure timely adoption of new technology the assessment team recommends that new versions of technologies and standards that include fixes or patches for known vulnerabilities (as opposed to simply adding new functionality) should be adopted within 30 days of their publication. | Subcommittees should consider standard(s) to require the implementation of fixes or patches for known vulnerabilities within 30 days of their publication as recommended. | Modified standards to specify specific timelines where applicable, and in all other cases make change as soon as possible in coordination with trading partners.**WGQ**:D2, D3, D5, D6, D32, D34**RMQ**:D4, D7, D8 |
| Two | Business Operations Practices and Standards Report Section 6.1.1 – NAESB Standards Refer to Vulnerable Versions of Communication Protocols (Pages 10 – 11) | Level: HighSince existing systems may not be compatible with updated software packages or protocol versions, updates may be too expensive to utilize, or for other business related decisions, the assessment team recommends the owning organization notify their trading partners of any systems or software that have not been updated and the potential impact of utilizing the vulnerable system in the 30-day window. This allows business partners to assess the risk of conducting business over those legacy systems. | Subcommittees should consider standard(s) to provide notice to trading partners as recommended | Modified standards to specify specific notification timelines where applicable, and in all other cases make change as soon as possible in coordination with trading partners. **WGQ:**D2, D3, D5, D6**RMQ:** D4, D7, D8. |
| Three | Business Operations Practices and Standards Report Section 6.1.1 – NAESB Standards Refer to Vulnerable Versions of Communication Protocols (Pages 10 – 11) | Level: HighAll the communications standards specified in the Internet Electronic Transport (IET) standards and the Electronic Delivery Manual (EDM) for Retail Gas Quadrant and Retail Electric Quadrants. The assessment team recommends that the NAESB review and upgrade the minimum requirement for SSL/TLS to version 1.2 configured with FIPS-based cipher suites as a minimum[[1]](#footnote-1). NIST 800-52 details the TLS version and associated configurations and 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.  | Subcommittees should review TLS/SSL references and update the standard(s) accordingly as recommended | Modified standards to specify TLS V1.2, and centralized such references to make future revisions easier.**WGQ:**D10, D12, D14, D19, D28, D29, D30, D32, D34, D35, D36, D39, D40, D44**RMQ:**D20, D21, D26a, D26b, D36, D39, D40, D44 |
| Four | Business Operations Practices and Standards Report Section 6.1.1 – NAESB Standards Refer to Vulnerable Versions of Communication Protocols (Pages 10 – 11) | Level: HighIn addition, while implementation details are outside the purview of NAESB, the assessment team recommends adding a note that any major security bulletins or recommendations should, at the least, be considered for implementation within a 30-day window, even if a new version of the standard is not yet available or finalized. | Subcommittees should consider standard(s) with a recommended implementation window. | Modified standards to specify specific notification timelines where applicable, and in all other cases make change as soon as possible in coordination with trading partners. **WGQ:**D1, D2, D3, D5, D6**RMQ:**D4, D7 |
| Five | Business Operations Practices and Standards Report Section 6.1.2 – NAESB Standards Need Review for Unused or Unnecessary Functionality (Page 11) | Level: LowAs part of an annual review the analysis team recommends review of NIST 800-52 for guidance. Monitoring of required protocols as defined in WEQ-002.3 and the IET data dictionary tableupdates for acceptable configurations for supported secure communication protocols defined for IET are all recommended for immediate update as required by independent facility implementation based on NIST NVD, US CERT, ICS CERT or vendor mandate. The assessment team recommends any updates for these communication protocols to be considered for incorporation into standards following review as an updated minimum version 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, retail electric and retail gas quadrants should consider for incorporation as well. | As part of a recurring WGQ Annual Plan Item, the WGQ EDM Subcommittee reviews and updates the technical characteristics in WGQ EDM Manual Appendices B – D.Subcommittees should consider adding requirement to RMQ EDM Manual to state entities should seek to utilize the latest generally available version of protocols within 9 months of such version becoming available as recommended. | Modified our standards to include specific versions that should be observed. Not, however, that the “9 month GA” timeline is relevant to WGQ web sites standards; the RMQ has no corresponding web site standards.**WGQ:**N/A**RMQ:**D7, D8 |

| **Issue** | **Report Section (Page Number)** | **Sandia Finding or Consideration** | **Standard Considerations (if applicable)** | **Assignment (if applicable)** |
| --- | --- | --- | --- | --- |
| Seven | 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.[[2]](#footnote-2) 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. | Modified standards to include both specific and broad adoption of system security measures, and specific notification and coordination during outages with effected trading partners. **WGQ:**D3, D5**RMQ:**D4 |
| Nine | 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. | Modified our standards to both remove dated versions (specifically PGP) and centralized such references to make future revisions easier.**WGQ:**D15, D17, D37, D38, D46, D49, D51, D55, D57, D58, D60, D61**RMQ:**D15, D37, D38, D46, D49, D51, D55, D57, D58, D60, D61 |
| Ten | 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) | The assessment team recommends that updates within the IET standards to clarify language under the security section to NIST 800-52 details the TLS version and associated configurations and 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. NIST 800-52 disallows SSL implementation for both government and business – facing applications and as such, the assessment team recommends disallowing support for SSL version protocols and implement TLS version 1.2 as described. | The subcommittees should review TLS/SSL references and update the standard(s) accordingly as recommended (Already addressed as part of Issue #3) | Modified our standards to specify TLS V1.2, and centralized such references to make future revisions easier.**WGQ:**D10, D12, D14, D19, D28, D29, D30, D32, D34, D35, D36, D39, D40, D44**RMQ:** D20, D21, D26a, D26b, D36, D39, D40, D44 |
| Eleven | 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) | An HTTPS[[3]](#footnote-3) solution will protect information in transit, supporting overall privacy needs. Using basic authentication over HTTP is inherently insecure as username/password combinations are not encrypted in HTTP basic authentication[[4]](#footnote-4). If the communication channel is secured via HTTPS, then those credentials are secured as well. While self-signed certificates are acceptable for payload protection, HTTPS communication must be secured via certificates issued by a trusted, commercial certificate authority such as a NAESB ACA in order to verify certificate authenticity. Additional options for certificate authorities include commercial certificate authorities include IdenTrust, Comodo, GoDaddy, GlobalSign, and DigiCert; other valid certificate authorities exist as well. | Subcommittees should review standard(s) referencing HTTP/HTTPS (specifically WGQ Standards 4.3.60, 4.3.83, and 10.3.4 and RXQ Standard 7.3.4) and modify as needed.Subcommittees should consider standard(s) securing communications via certificates as recommended. | Modified our standards to specify HTTPS whenever secure communication is required.**WGQ:**D1, D9, D13, D16, D18, D27, D28, D29, D40, D45**RMQ:**D24, D25, D40, D45 |
| Twelve | 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[[5]](#footnote-5). 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[[6]](#footnote-6). | 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

Review and revise as recommended the WGQ EDM Manual (Page 90 – Security: Login and Encryption) requires 128-bit RSA JAVA communicationsThe RMQ EDM Manual does not specify anything RSA relatedThe WGQ IET Standards require a PGP version 2.6 or greater using RSA algorithm to generate keys (WGQ 10.3.15)The RMQ IET Standards require a RSA algorithm to generate keys and PGP Version 2.6 or greater (RXQ 7.3.15)Neither the WGQ/RMQ EDM or IET Standards address specifically address hash algorithms  | N/AJointly between WGQ EDM and RMQ IR/TEIS Modified standards to specify 128-bit key length, newer PGP versions and hash algorithms.**WGQ:**D12, D27, D53**RMQ:**D53 |
| Thirteen | 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[[7]](#footnote-7) and amplification[[8]](#footnote-8) 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 | ? |
| Four | 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. | The WGQ EDM Manual requires HTTP Basic Authentication or similar logon/password mechanisms for customer activity websites (WGQ 4.3.60) and accessing Interactive Flat File EDM (WGQ 4.3.84)The RMQ EDM Manual relies on the RMQ IET Standards for security principles, including authentication. (RXQ.5.6 Technical Implementation)The WGQ/RMQ IET Standards require basic authentication (WGQ.10.3.16 and RMQ.7.3.16) with the Security Sections (WGQ Page 20 and RMQ Page 14) specifically requiring 128-bit SSL-protected usernames and passwords to establish authentication and list optional techniques such as firewall security for further authentication. | Modified standards to to state that secure web sites should employ individual user credentials. However, we find that the current standard of user IDs and passwords maintains the security of web sites without complicating the login process, especially for users that access multiple web sites.**WGQ:**D1, D9, D18, D29, D40, D45**RMQ:**D40, D45 |
| Ten | Addendum Report Section 3.4 – Recommended Future Assessments (Pages 29 – 30) | Perform security assessments on applicable software, services or platforms (SSP’s). Also according to SANS: “Security assessments should be performed on all externally-accessible SSPs for all new or major application releases. All point releases, patch releases, etc. should be subject to the appropriate level of assessment needed based on the level of risk the change posed to the application but at a minimum, annually.” The assessment team recommends that the software vendors, in partnership with their customers, determine the specifics of these assessments to ensure that all relevant risks are addressed. | Subcommittees should review EDM and IET Standards to determine if there are areas where additional language could be added recommending customers and software vendors work together as recommended | Modified standards to encourage security assessments and coordination between customers, vendors and trading partners.**WGQ:**D1, D32, D33, D34**RMQ:** N/A |

1. **Business Purpose:**

To establish needed modifications to the NAESB RMQ Model Business Practices based on the results of the Sandia National Laboratories surety assessment as proposed by the NAESB Board Critical Infrastructure Committee.

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

The RMQ IR/TEIS and WGQ EDM Subcommittee held 8 joint conference calls on the following dates:

[August 19, 2019](https://www.naesb.org/pdf4/wgq_edm_retail_ir_teis081919fm.doc)

[August 26, 2019](https://www.naesb.org/pdf4/wgq_edm_retail_ir_teis082619fm.doc)

[September 9, 2019](https://www.naesb.org/pdf4/wgq_edm_retail_ir_teis090919fm.doc)

[September 23, 2019](https://www.naesb.org/pdf4/wgq_edm_retail_ir_teis092319fm.doc)

[October 9, 2019](https://www.naesb.org/pdf4/wgq_edm_retail_ir_teis100919fm.doc)

October 23, 2019

November 11, 2019

December 2, 2019

During the December 2, 2019 joint WGQ EDM and RMQ IR/TEIS conference call, this RMQ recommendation was unanimously approved.

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. NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS) <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf> [↑](#footnote-ref-2)
3. *Securing the Web*, retrieved on June 10, 2019, from <https://www.w3.org/2001/tag/doc/web-https> [↑](#footnote-ref-3)
4. RFC 2617: *HTTP Authentication: Basic and Digest Access Authentication*, retrieved on June 10, 2019, from <https://tools.ietf.org/html/rfc2617> [↑](#footnote-ref-4)
5. 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-5)
6. Symantec Corporation. *PGP Command Line 9.0 User’s Guide*. Symantec, 2006. [↑](#footnote-ref-6)
7. *Replay Attacks*, retrieved on June 10, 2019, from <https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/replay-attacks> [↑](#footnote-ref-7)
8. *DNS Amplification Attacks*, retrieved on June 10, 2019, from <https://www.us-cert.gov/ncas/alerts/TA13-088A> [↑](#footnote-ref-8)