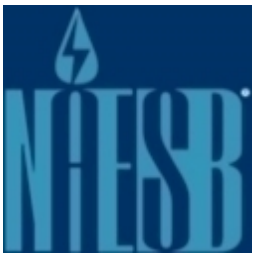
Assessment Report of the North American Energy Standards Board Business Operations Practices and Standards

24 June 2019

Prepared for the Department of Energy and

North American Energy Standards Board



Prepared By

Information Design Assurance Red Team
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185

Acknowledgements

This document was prepared for the Department of Energy (DOE), Office of Fossil Energy by a working group of the Information Design Assurance Red Team (IDART™) at Sandia National Laboratories (SNL). The working group had the following members:

Benjamin Anderson, Project Lead
Sandia National Laboratories
Cyber Systems Security R&D
505-844-9345
brander@sandia.gov

Joshua Daley, IDART Analyst
Sandia National Laboratories
Cyber Systems Security R&D

Ryan Kao, IDART Analyst
Sandia National Laboratories
Autonomous Cyber Systems

Marshall Riley, IDART Analyst
Sandia National Laboratories
Cyber Systems Security R&D

The working group would like to thank the following individuals from the North American Energy Standards Board (NAESB) for their contribution to this document:

Rae McQuade, Executive Director
Jonathan Booe, Executive Vice President & Chief Administrative Officer
Caroline Trum, Deputy Director

In addition, the working group would like to thank the following individuals for supporting the IDART working group meeting held at the NAESB Office in Houston on August 3, 2017:

Jim Buccigross, 8760, Inc.
Christopher Freitas, Department of Energy
Lancen LaChance, GlobalSign
Paul Sorenson, OATI
Leigh Spangler, Latitude Technologies

This page intentionally left blank.

Table of Contents

Executive Summary

The North American Energy Standards Board (NAESB) was formed in 1994 with the support of the Department of Energy (DOE). The purpose of NAESB is to streamline transactions in the natural gas and electric industries by developing voluntary standards and model business practices. These standards and practices are used by participants in the wholesale and retail aspects of the gas and electric markets.

This report provides an analysis of multiple NAESB standards and business practices related to Internet electronic transport, and quadrant electronic delivery mechanisms. The assessment team used the Information Design Assurance Red Team (IDART™) methodology to conduct the analysis and assessment of the business operations practices and standards[1].

This assessment was executed by the Information Design Assurance Red Team (IDART™) at the request of program manager, Mr. Christopher Freitas, of the Department of Energy (DOE), Office of Fossil Energy, Office of Oil and Natural Gas. The intent is to provide a surety assessment of selected NAESB standards related to Internet electronic transport and quadrant electronic delivery mechanisms.

The cooperation and assistance given to IDART by NAESB and their partner organizations was greatly appreciated and was critical to making this surety assessment possible.

The analysis showed that the NAESB Standards and Business Practices related to Internet Electronic Transport and Quadrant Electronic Delivery provide a solid foundation to ensure that electronic communications can be conducted in a reliable and secure manner. The main vulnerabilities were related to the maintenance and updating of NAESB Standards and Business Practices. Specifically, the team identified the following:

- NAESB Standards refer to vulnerable versions of communication protocols and should reference the latest versions of technology or protocol standards
- NAESB Standards include unused or unnecessary functionality, and should be reviewed to determine what functionality can be deprecated or removed

Overall, the assessment team feels that, while these vulnerabilities pose a risk to business and control operations, they should already be addressed if organizations are utilizing industry best practices in their implementation of NAESB Standards.

[1] Information on the IDART Methodology can be found at: http://idart.sandia.gov/

1 Introduction

The North American Energy Standards Board (NAESB) was formed in 1994 with the support of the Department of Energy (DOE). The purpose of NAESB is to streamline transactions in the natural gas and electric industries by developing voluntary standards and model business practices. These standards and practices are used by participants in the wholesale and retail aspects of the gas and electric markets.

This report provides an analysis of multiple NAESB standards and business practices related to Internet electronic transport, and quadrant electronic delivery mechanisms. The assessment team used the Information Design Assurance Red Team (IDART™) methodology to conduct the analysis and assessment of the business operations practices and standards[2].

The assessment team operated on the principle that an independent analysis should include a comprehensive assessment and suggested improvements, while incorporating surety engineering concepts throughout the activity. The team defined surety as a measure of the assurance of system reliability, safety, security, and control of use, while balancing denial of unauthorized use with assurance of authorized use within the constraints of risk versus cost.

This assessment was executed by the Information Design Assurance Red Team (IDART™) at the request of program manager, Mr. Christopher Freitas, of the Department of Energy (DOE), Office of Fossil Energy, Office of Oil and Natural Gas. The intent is to provide a surety assessment of selected NAESB standards related to Internet electronic transport and quadrant electronic delivery mechanisms.

This task involved a review of the following NAESB documents:

- Internet Electronic Transport Related Standards, Version 3.0
- RXQ.7 – Internet Electronic Transport Model Business Practices, Version 3.1
- WGQ Quadrant Electronic Delivery Mechanism Related Standards, Version 3.0
- RXQ.5 – Quadrant-Specific Electronic Delivery Mechanism Model Business Practices, Version 3.1

2 Objective and Purpose of the NAESB Business Operations Standards

The use of the Internet for electronic commerce requires standards that enable reliable and secure communication between organizations. To support this need, NAESB has developed standards for the Wholesale Gas Quadrant (WGQ), Retail Electric Quadrant (REQ), and Retail Gas Quadrant (RGQ). These standards enable the rapid, reliable, and safe transportation of electronic information between NAESB trading partners.

The NAESB standards and business practices:

- Provide a high-level guide to implementing various technologies necessary for this communication

[2] Information on the IDART Methodology can be found at: http://idart.sandia.gov/

- Establishes a framework for the electronic dissemination and communication of information between parties in the retail gas and electric marketplaces (REQ and RGQ)
- Standardizes methods of communication that can be implemented by trading partners
- Provide business benefits by providing open standards that can be used with partners outside of the WEQ, REQ, and RGQ areas
- Specifies what functions each party should perform in electronic transactions, including functions such as establishing an audit trail and notifying other parties of any errors detected

Combined, these standards and business practices define a reliable and secure method of communication between trading partners, which allows them to conduct business operations over the Internet.

3 Critical Success Factors

Factors which are critical to the success of the Business Operations Practices and Standards were identified during the analysis of the documents listed in Section 1. These factors are crucial in determining the effectiveness of the various standards in providing a reliable and secure method of communication between trading partners. Critical success factors identified include the following:

- Trading partners act in good faith when it comes to implementing NAESB requirements and performing relevant functions (such as reporting errors)
- Trading partners use appropriate cyber security practices within their organizations to ensure that proprietary or business information shared by their trading partners is not compromised
- Compromises of information are accurately reported to affected trading partners, NAESB, an ACA, or other interested parties in a timely manner consistent with NAESB and ACA requirements

4 Metrics of Importance

Metrics should be collected and analyzed to measure how the implementation of the Business Operations Practices and Standards increases the reliability and security of electronic data exchanged between trading partners. The following are some examples of metrics that could be collected for NAESB and industry partners to review and analyze:

- 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 best, median, average, and worst time for a transaction to be completed
- Count the number of organizations that have established continuity of operations planning (COOP), and the number of organizations that exercise their COOP each year
- Count the number of organizations that maintain alternate and 24/7 contact information for trading partners, and the number that have this information stored offline (in case of a ransomware attack)

- Count the number of times alternate methods were used for transactions (ex. phone or fax) during normal operations; and during a system outage, failure, or other issue

These metrics could be self-reported – either to NAESB or maintained by each organization on a statistics webpage that can be accessed by their trading partners. If desired, NAESB could collect and tabulate the totals on a monthly basis, 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, analysis of COOP and disaster recovery plans, and determining if NAESB standards need to be upgraded or revised.

5 Surety Assessment Research

Research of the NAESB Business Operations Practices and Standards began with the assessment team reviewing the following NAESB documents:

- Internet Electronic Transport Related Standards, Version 3.0
- RXQ.7 – Internet Electronic Transport Model Business Practices, Version 3.1
- WGQ Quadrant Electronic Delivery Mechanism Related Standards, Version 3.0
- RXQ.5 – Quadrant-Specific Electronic Delivery Mechanism Model Business Practices, Version 3.1

These standards also refence multiple documents and standards, including multiple Internet Engineering Task Force (IETF) requests for comment (RFCs). These included RFCs related to OpenPGP (RFC 2440), HTTPS/SSL (RFC 2246), and MIME (RFCs 2045, 2046, 2047, 2048, 2049). In addition, industry standards such as ASC X.12 were also referenced. These, and other reference documents were reviewed by the assessment team to provide context for the information in the NAESB Standards.

From a high-level view, the assessment team found two areas of concern. The first area is referencing specific versions of a protocol or technology, which may not be the latest version. This is a concern since protocols may be updated to address new vulnerabilities or adversary capabilities and the referenced version may be vulnerable to attack. The second area is the inclusion of legacy or deprecated functionality. Since it is impossible to know what capabilities adversaries will develop in the future, any functionality could provide an attack vector for malicious activity. Therefore, if functionality is not being used, it should be removed to prevent an adversary from discovering a vulnerability in the future.

6 Surety Assessment Analysis and Recommendations

This analysis focused on the use of various technologies (ex. PGP encryption) and the standards and business practices utilized by trading partners to exchange electronic information. The assessment team recommends that NAESB review their standards and perform any updates to address the findings listed in this section.

6.1 Security Issues

Items listed in this section deal specifically with vulnerabilities that could provide an opportunity to an attacker wishing to conduct malicious activities that would affect business operations that utilize the NAESB Standards related to Internet Electronic Transport standards and business practices, as well as those for Quadrant Electronic Delivery Mechanisms standards and business practices.

For the level of severity: A HIGH value represents a systemic weakness which could allow an adversary to directly and/or covertly conduct malicious activity. A MODERATE value represents a weakness which could allow an adversary to conduct malicious activity and cause considerable degradation of operations. A LOW value represents a weakness which could allow an adversary to conduct malicious activity and cause targeted or limited impact on the mission.

6.1.1 NAESB Standards Refer to Vulnerable Versions of Communication Protocols

NAESB standards contain references to specific versions of communication protocols that may be vulnerable to attacks discovered since the publication of those standards. For example, the standards require the use of the Secure Sockets Layer (SSL) protocol, which has been replaced by the Internet Engineering Task Force (IETF) with the Transport Layer Security (TLS) protocol. For reference, a table listing the locations of SSL references in the reviewed documents can be found in Section 10 (Appendix B).

Level: HIGH

Analysis: Insecure protocols can allow an attacker to intercept or modify communications, or to impersonate the various parties involved in the communication.

Recommendation: In 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.

Since 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.

All 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[3]. 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,

[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

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. No other findings were noted in the review of the communication standards specified in WEQ-002.

In 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.

6.1.2 NAESB Standards Need Review for Unused or Unnecessary Functionality

NAESB standards contain legacy or deprecated functionality.

Level: LOW

Analysis: As electronic communication standards evolve at a rapid rate, functionality that was necessary to ensure accurate communications can become unnecessary. The assessment team did not identify any vulnerabilities in the standards they reviewed but did identify optional fields in the WGQ/REQ/Internet Electronic Transport Related Standards that could prove to be an attack vector in the future. The fields that are identified by the IET data dictionary as mutually agreed (not mandatory) are time-c qualifier, and refnum, refnum-orig, and transaction-set. As part of the annual review the assessment team recommends a survey review for these data fields that may no longer be utilized to determine if they data fields can be removed. Unused data fields can be leveraged to cause undefined system states that can lead to unwanted system behavior.

Recommendation: As 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 table updates 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.

6.1.3 Strengths of the NAESB Business Operations Practices and Standards

This section details areas that the assessment team identified as practices or requirements that prevented or increased the difficulty of a successful attack or exploitation by an adversary. These are specifically enumerated to ensure that such practices are continued as the target system evolves.

6.1.4 Use of Human Control and Review in Operations

Currently, business and control operations are performed or authorized by an individual who is familiar with normal operations. For example, business operations for a specific trading partner is generally assigned to a specific individual who oversees all interactions with that partner. This allows the human to note abnormal behavior and communicate with the trading partner to determine if the operations are accurate.

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.[4] 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.

6.1.5 Separation of Business and Control Computer Networks

The EDI cyber attack that occurred in April 2018 illustrated the importance of maintaining separation of business and control networks. While the cyber attack against the EDI platform interrupted business functions, COOP procedures were utilized, and it was possible for the affected organizations to continue operations. If the control networks and business networks were connected, it is possible that the cyber attack would have prevented pipeline operations.

In recent years, Supervisory Controls and Data Acquisition (SCADA), process control and industrial manufacturing systems have increasingly relied on commercial information technologies for both critical and non-critical communications. While beneficial in other areas, use of these common protocols and operating systems has resulted in increased connectivity from the outside world for vital SCADA and Process Control Networks (PCNs). These systems are now under risk of attack from a variety of threats.

Some commonly suggested security solutions are to isolate the SCADA and PCN systems from the Internet and corporate enterprise network (EN) through the use of firewalls, which can be complex devices to design and deploy correctly, data diode separation which allows network data to flow in one direction allowing for monitoring of control systems but not allowing control signals to traverse from the business side network to the control network, virtual private network implementation which restricts access to designated portions of the network, internet protocol security (IP sec) which is a protocol implementation designed to require encryption between two devices and requires a shared public key.

[4] NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS)
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

This Centre for the Protection of National Infrastructure (CPNI) Good Practice document addresses the need for guidance in creating such firewalls. There are a significant number of different solutions used by the industry and the security effectiveness of these can vary widely. In general, architectures that allow the establishment of a Demilitarized Zone (DMZ) between the enterprise network and SCADA/PCN network will provide the most effective security solution. Realize this part of defense-in-depth strategy. Here is more complete treatment [5]

Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, Industrial Control Systems Cyber Emergency Response Team, September 2016.

6.1.6 Continued Use of Different Security Paradigms

Despite the increased connectivity between the gas and electric markets, both markets have continued to use their original security paradigms – PGP-based or PKI-based encryption. Both systems provide a high-level of surety in establishing and maintaining a secure and reliable communication channel between partners.

The assessment team feels that, since both approaches provide for secure communications, each market should continue using their mature systems instead of all markets switching to a common technology. Mature systems have generally had usability and security issues identified, proper configurations established, and have provided a stable environment for their administrators to gain experience with the technologies. A switch to a different technology could result in vulnerabilities as system owners and administrators work to gain experience with and deploy the new systems.

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.

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. An HTTPS[6] solution will protect information in transit, supporting overall privacy needs. Using basic authentication over HTTP is inherently insecure as username/password combinations are not

[5] (https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf)

[6] *Securing the Web*, retrieved on June 10, 2019, from https://www.w3.org/2001/tag/doc/web-https.

encrypted in HTTP basic authentication[7]. 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. .

Key lengths must be updated to reflect current acceptable encryption strength[8]. 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[9].

Finally, IET business process as currently implemented may be vulnerable to both replay[10] and amplification[11] attacks. Based on the assessment teams review of the transactional process these two attacks were immediately identified as attacks of concern. First, requests are not sent with a trustworthy transaction identifier in the envelope. As a result, an attacker who can acquire a man-in-the-middle position can intercept requests and replay them to a server at a later date. Without a transaction identifier, the receiver would have no way to determine if that request is new or old and would therefore process the request. This vulnerability is mitigated through the unique identifier assigned by the transmission services information provider (TSIP). An envelope-based identifier if used must be digitally signed by the sender to be trustworthy.

Amplification attacks use generated responses from a trusted host to execute denial of service attacks. In this case, an adversary can execute an attack against a spoofed sender by sending deliberately mis-formatted payload data to receivers. The adversary needs to, first, spoof the identification information of the sender and the IP address of the target or receiver so the receiver believes the request is valid and from the spoofed sender. Then, the adversary needs to craft a small, mis-formatted payload and send that payload in a request message. The receiver will respond with a signed gisb-acknowledgement-receipt response and close the connection when all message data has been received. The payload is

---

[7] RFC 2617: *HTTP Authentication: Basic and Digest Access Authentication*, retrieved on June 10, 2019, from https://tools.ietf.org/html/rfc2617.

[8] Barker, E. and Roginsky, A. NIST 800-131A: *Transitioning the Use of Cryptographic Algorithms and Key Lengths*. National Institute of Standards and Technology, 2019.

[9] Symantec Corporation. *PGP Command Line 9.0 User's Guide*. Symantec, 2006.

[10] *Replay Attacks*, retrieved on June 10, 2019, from https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/replay-attacks.

[11] *DNS Amplification Attacks*, retrieved on June 10, 2019, from https://www.us-cert.gov/ncas/alerts/TA13-088A.

then decrypted and processed, and when an error is found, an ET Error Notification message is sent to the spoofed sender. This notification message is larger than the submitted request. This can amplify a denial-of-service attack significantly as an attacker can craft a small, corrupted request, submit it to a server, and the server will then send the spoofed client the larger error notification message. 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.

This is not to imply that new vulnerabilities or business needs should be ignored in the adoption of different technologies; however, the assessment team wants to ensure that organizations consider the risks in replacing existing, stable, and secure systems with new technology

7 Summary

The assessment team conducted an analysis of the NAESB Business Operations Practices and Standards, which included the following documents:

- Internet Electronic Transport Related Standards, Version 3.0
- RXQ.7 – Internet Electronic Transport Model Business Practices, Version 3.1
- WGQ Quadrant Electronic Delivery Mechanism Related Standards, Version 3.0
- RXQ.5 – Quadrant-Specific Electronic Delivery Mechanism Model Business Practices, Version 3.1

The cooperation and assistance given to IDART by NAESB and their partner organizations was greatly appreciated and was critical to making this surety assessment possible.

The analysis showed that the NAESB Standards and Business Practices related to Internet Electronic Transport and Quadrant Electronic Delivery provide a solid foundation to ensure that electronic communications can be conducted in a reliable and secure manner. The main vulnerabilities were related to the maintenance and updating of NAESB Standards and Business Practices. The following strengths of the NAESB Standards were identified:

- The use of human control and review in conducting operations
- The separation of the business and control computer networks

The following weaknesses in the security of the Business Operations and Practices were identified:

- NAESB Standards refer to vulnerable versions of communication protocols and should reference the latest versions of technology or protocol standards
- NAESB Standards include unused or unnecessary functionality, and should be reviewed to determine what functionality can be deprecated or removed

Overall, the assessment team feels that, while these vulnerabilities pose a risk to business and control operations, they should already be addressed if organizations are utilizing industry best practices in their implementation of NAESB Standards. However, to ensure that all organizations are using the most secure implementations of technologies and protocols, the assessment team recommends NAESB updates their documents to reference any updated standards.

8 Conclusion

This report is intended to contribute to the improve of NAESB Business Operations Practices and Standards and identify any vulnerabilities that could pose a risk to business operations in the electric and natural gas markets, and was developed with the best information available at the time of the assessment.

Overall, the assessment team found that the NAESB Standards and Business Practices related to Internet Electronic Transport and Quadrant Electronic Delivery provide a solid foundation to ensure that electronic communications can be conducted in a reliable and secure manner. However, the team recommends that NAESB performs some minor updates to their Standards and Business Practices to address the issues discussed in Section 6 to ensure that all organizations are using the most secure versions of technologies and protocols that are available.

9 Appendix A: Abbreviations and Acronyms

ACA	Authorized Certificate Authority
CA	Certification Authority
COOP	Continuity of Operations Planning
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DOE	Department of Energy
FE	Office of Fossil Energy
IDART	Information Design Assurance Red Team
IETF	Internet Engineering Task Force
NAESB	North American Energy Standards Board
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
PKI	Public Key Infrastructure
REQ	Retail Electric Quadrant
RFC	Request for Comment
RGQ	Retail Gas Quadrant
SNL	Sandia National Laboratories
WEQ	Wholesale Electricity Quadrant

10 Appendix B: References to SSL Protocol in Reviewed Documents

This section contains the list of references to SSL found in the documents reviewed by the assessment team. It does not include references to SSL if they are included as a definition, a cross reference between NAESB standards, or as part of a modifications list.

Document Title	Page(s) With Reference
Internet Electronic Transport Related Standards, Version 3.0	5, 20 (x2), 26, 33
RXQ.7 – Internet Electronic Transport Model Business Practices, Version 3.1	7, 14 (x2), 22, 30, 70
WGQ Quadrant Electronic Delivery Mechanism Related Standards, Version 3.0	46, 49, 73 (x2), 90, 96 (x6), 99
RXQ.5 – Quadrant-Specific Electronic Delivery Mechanism Model Business Practices, Version 3.1	12, 15, 21, 29, 35
WEQ-012 Public Key Infrastructure, Version 003.1	NONE
Accreditation Requirements for Authorized Certification Authorities – February 18, 2014	4 (x3)
NAESB Authorized Certification Authority Process – December 8, 2016	NONE
WEQ-001 Open Access Same-Time Information Systems (OASIS)	NONE
WEQ-002 OASIS Standards and Communication Protocols	6, 104 (x3), 105 (x2)[12]
WEQ-003 OASIS Data Dictionary	NONE
WEQ-013 OASIS Implementation Guide	NONE

[12] This document does refer to SSL/TLS, but includes a reference to an insecure version of the TLS protocol.

11 Appendix C: Relevant Document Summary Table

This section summarizes the documents, standards, or business practices – and the relevant section(s) – where any identified issues are located. Also included is a column with the corresponding section from this report that discusses the identified issue.

Table 1: References to SSL or Previous TLS Versions

Relevant Source Document	Relevant Page(s) and Number of Occurrences per Page	Location in This Report
Internet Electronic Transport Related Standards, Version 3.0	5, 20 (x2), 26, 33	Section 6.1.1
RXQ.7 – Internet Electronic Transport Model Business Practices, Version 3.1	7, 14 (x2), 22, 30, 70	Section 6.1.1
WGQ Quadrant Electronic Delivery Mechanism Related Standards, Version 3.0	46, 49, 73 (x2), 90, 96 (x6), 99	Section 6.1.1
RXQ.5 – Quadrant-Specific Electronic Delivery Mechanism Model Business Practices, Version 3.1	12, 15, 21, 29, 35	Section 6.1.1
Accreditation Requirements for Authorized Certification Authorities – February 18, 2014	4 (x3)	Section 6.1.1
WEQ-002 OASIS Standards and Communication Protocols	6, 104 (x3), 105 (x2)[13]	Section 6.1.1

[13] This document does refer to SSL/TLS, but includes a reference to an insecure version of the TLS protocol.

Table 2: References to "refnum"

Relevant Source Document	Relevant Page(s)	Location in This Report
Internet Electronic Transport Related Standards, Version 3.0	30, 32, 33, 35, 57, 58	Section 6.1.2
RXQ.7 – Internet Electronic Transport Model Business Practices, Version 3.1	26, 28, 29, 32, 57, 58, 65	Section 6.1.2
WGQ Quadrant Electronic Delivery Mechanism Related Standards, Version 3.0	14[14]	Section 6.1.2
RXQ.5 – Quadrant-Specific Electronic Delivery Mechanism Model Business Practices, Version 3.1	33, 34	Section 6.1.2

Note: The above table does not include the number of occurrences on each page as the sections are expected to be removed instead of updated.

[14] Only included as a reference to request R01019