**DRAFT**

North American Energy Standards Board

Response to Sandia National Laboratories Surety Assessment

Prepared by the NAESB Critical Infrastructure Committee

*Presented to the NAESB Board of Directors on April 23, 2020*

|  |
| --- |
| **NORTH AMERICAN ENERGY STANDARDS BOARD****RESPONSE TO SANDIA NATIONAL LABORATORIES SURETY ASSESSMENT****TABLE OF CONTENTS** |
|  | Page |
| I. | Executive Summary | 3 |
| II. | Surety Assessment Development | 3 |
| III. | NAESB Response | 7 |
| IV. | Conclusion | 9 |
| Appendices  | A. | Surety Assessment Recommendations to Mitigate Security Issues and NAESB Responses | 11 |
|  | B. | Surety Assessment Additional Findings for NAESB Consideration and NAESB Responses | 18 |

**I. Executive Summary**

This report was prepared by the North American Energy Standards Board (NAESB) Critical Infrastructure Committee to communicate the efforts taken by the organization in response to the surety assessment performed by Sandia National Laboratories. The purpose of the surety assessment, funded by the U.S. Department of Energy (DoE), was to analyze cybersecurity elements within the NAESB Business Practice Standards and Model Business Practices. This is the third such assessment on the NAESB standards sponsored by the U.S. DoE and conducted by Sandia National Laboratories. Both previous assessments, conducted in 2000 and 2006, respectively, resulted in recommendations that led to modifications of the NAESB Business Practice Standards and Model Business Practices. Included in this report is an overview of the recommendations and findings made by Sandia National Laboratories, a summary of the resulting standard development efforts and standard changes, and a description of the actions underway to address any remaining items identified by Sandia National Laboratories for further consideration by NAESB.

NAESB is a 501(c)(6) non-profit entity accredited by the American National Standards Institute (ANSI) as an ANSI Standards Development Organization. NAESB originated as the Gas Industry Standards Board in 1994 and was formed by the industry with the support of the U.S. DoE and the Federal Energy Regulatory Commission (FERC). The voluntary, consensus-based standards and model business practices developed by NAESB serve to streamline the transactional processes of the natural gas and electric industries by promoting more competitive and efficient services in the wholesale and retail gas and electric markets. A fundamental element of the NAESB Business Practice Standards and Model Business Practices is the inclusion of cybersecurity best practices to assist in the secure transmission of electronic business transactions. As a result of the recommendations and additional findings made by Sandia National Laboratories, NAESB has not only undertaken standards development to help ensure the standards and model business practices continue to provide cybersecurity protections to address the current needs of the gas and electric industries but also has activities underway to consider the processes the organization could employ to meet the future cybersecurity needs of both industries.

NAESB would like to take this opportunity to express thanks for the continued support of the U.S. DoE since the organization’s inception over two decades ago. Specifically, NAESB is appreciative of the U.S. DoE’s Office of Fossil Energy for sponsoring this third surety assessment of the NAESB Business Practice Standards and Model Business Practices as well as Christopher Freitas for shepherding the process on behalf of the U.S. DoE. NAESB looks forward to continuing to work with the U.S. DoE on activities that support the energy industry.

**II. Surety Assessment Development**

In April 2017, NAESB announced that Sandia National Laboratories, through funding provided by the U.S. DoE, would be performing a surety assessment to analyze cybersecurity elements of the NAESB Business Practice Standards and Model Business Practices. As determined by Sandia National Laboratories and the U.S. DoE, the surety assessment focused on four areas: (1) an assessment of the NAESB Certification Program for Accredited Certification Authorities, including the Wholesale Electric Quadrant (WEQ) Public Key Infrastructure Business Practice Standards, the NAESB Accreditation Requirements for Authorized Certificate Authorities, and the Authorized Certification Authority Process; (2) an assessment of the of the WEQ Open Access Same-Time Information System (OASIS) Suite of Business Practice Standards; (3) an assessment of the Wholesale Gas Quadrant (WGQ) and Retail Markets Quadrant (RMQ) Internet Electronic Transport (IET) and Electronic Delivery Mechanism (EDM) Business Practice Standards/Model Business Practices; and (4) a high-level dependency analysis between the gas and electric markets.

The NAESB Certification Program for Accredited Certification Authorities supports cybersecurity protections for commercial transactions within the wholesale electric market. The certification program allows certificate authorities to become authorized to issue digital certificates under the WEQ-012 Public Key Infrastructure Business Practice Standards. These standards establish a comprehensive cybersecurity framework that enables secure electronic commercial transactions via data encryption and party authentication through the use of digital certificates issued by a NAESB Authorized Certificate Authority (ACA). The other requirements for the certification program are defined by the NAESB Accreditation Requirements for Authorized Certificate Authorities, which establishes the technical requirements a NAESB ACA must meet in issuing a digital certificate, and the Authorized Certification Authority Process, which describes how a certificate authority can become a NAESB ACA. The NAESB WEQ Business Practice Standards require the use of a digital certificate issued by a NAESB ACA for all parties (1) accessing a transmission provider’s OASIS node – an industry tool that facilitates the scheduling of transmission service on the bulk power grid; (2) participating in communications regarding the electronic facilitation of interchange transactions through electronic tagging; and (3) accessing the NAESB Electric Industry Registry – an industry tool that serves as the central repository for information needed to support commercial scheduling and transmission management operations for the wholesale electric industry.

The WEQ OASIS Suite of Business Practice Standards (WEQ-001 OASIS Business Practice Standards, WEQ-002 OASIS Standards and Communication Protocols Business Practice Standards, WEQ-003 OASIS Data Dictionary Business Practice Standards, and WEQ-013 OASIS Implementation Guide Business Practice Standards) support the industry use of OASIS by supporting FERC posting and reporting requirements and establishing consistent implementation methods. Public utilities are required by FERC regulations to maintain an OASIS node for the purpose of scheduling transmission on the bulk electric power grid and making available to all transmission users comparable interactions with transmission service information. The OASIS system is comprised of the computer systems, associated communication facilities, and back-end supporting systems or user procedures that collectively perform the transaction processing functions associated with the handling of requests for transmission service on OASIS. The WEQ-001 OASIS Business Practice Standards define the general and specific transaction and business processing requirements. The WEQ-002 OASIS Standards and Communication Protocols Business Practice Standards detail requirements for network architecture and information access. The WEQ-003 OASIS Data Dictionary Business Practice Standards define the data element specifications for the OASIS nodes. The WEQ-013 OASIS Implementation Guide Business Practice Standards detail requirements related to implementation of the standards.

The WGQ and RMQ IET and EDM Business Practice Standards/Model Business Practices define the electronic communication framework, including cybersecurity protections, for commercial transactions within the wholesale gas and retail markets. For both wholesale gas and retail, the EDM Standards/Model Business Practices establish the framework for the electronic dissemination of information between parties. Within the retail markets, the model business practices address two standardized methods of communication: Electronic Data Interchange (EDI)/EDM Transfers and Flat Files/EDM Transfers. Within the wholesale gas market, the standards address five standardized methods of communication: EDI/EDM Transfers, Batch Flat File/EDM Transfers, Informational Postings Web Sites, Electronic Bulletin Boards/EDM, and Interactive Flat File/EDM. Both the model business practices and standards provide a high-level guide to the development, implementation, and testing of the communication methods. This includes defining the protocols, security, and transmission requirements for each method. The WGQ and RMQ IET Business Practice Standards/Model Business Practices define requirements for the implementation of technologies necessary to electronically communicate transactions and other data between trading partners, including security guidelines that address data privacy, data integrity, authentication, and non-repudiation.

NAESB worked closely with Sandia National Laboratories and representatives from the U.S. DoE throughout the surety assessment process. In August 2017, NAESB hosted a meeting between the Sandia National Laboratories surety assessment team and subject matter experts in the NAESB Business Practice Standards and Model Business Practices. The purpose of this meeting was to review and discuss the areas being addressed as part of the assessment and provide a broader understanding of how the gas and electric industries utilize the standards. It was as a result of discussions during this meeting that the surety assessment was expanded to include elements of the WEQ OASIS Suite of Business Practice Standards.

Additionally, in May 2017, the Chair of the NAESB Board of Directors reconvened the NAESB Critical Infrastructure Committee for the purpose of monitoring cybersecurity and critical infrastructure activities, specifically the surety assessment. The NAESB Critical Infrastructure Committee held eleven meetings between May 2017 and July 2019 to discuss the surety assessment. As part of these meetings, Sandia National Laboratories provided the opportunity for the committee to review the five draft iterations of the surety assessment reports and offer written feedback regarding the development of the final reports. This collaborative process, which included participation by the surety assessment team and U.S. DoE representatives in Board Critical Infrastructure Committee meetings as well as frequent communications at a staff level between NAESB, Sandia National Laboratories, and the U.S. DoE, resulted in the final reports submitted to NAESB

On July 22, 2019, Sandia National Laboratories provided NAESB with the final surety assessment reports:

(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

(4) Addendum Report: Threat-based Examination of NAESB Standards and Business Operations

Within each of the three assessment reports, Sandia National Laboratories identified two potential Security Issues, for a total of six potential Security Issues, and provided recommendations to mitigate each of the identified issues. For each of the six potential Security Issue, Sandia National Laboratories assigned a level of severity for the 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. Apart from the six potential Security Issues, the three assessment reports and the single addendum report include twenty-two Additional Findings made by Sandia National Laboratories for further consideration by NAESB. Unlike the potential Security Issues, these Additional Findings were not to address a potential vulnerability but rather identified additional considerations for NAESB to explore undertaking or general recommendations regarding future cybersecurity needs for the gas and electric industries.

As part of the Assessment Report of the NAESB Public Key Infrastructure Program, Sandia National Laboratories identified two potential Security Issues. These vulnerabilities were classified as Low level severity, and both involved minor discrepancies between the requirements established by the NAESB Public Key Infrastructure Program and the individual practices of the NAESB ACAs. Additionally, Sandia National Laboratories made three Additional Findings recommending the establishment of metrics to analyze how the implementation of the NAESB Public Key Infrastructure Program increases security and reliability of electronic data exchanges as well as best practices to ensure the continued security of digital certificates issued by NAESB ACAs.

As part of the Assessment Report of the NAESB OASIS Standards, Sandia National Laboratories identified two potential Security Issues. Both vulnerabilities were classified as Low level severity. These items addressed the possibility of a malicious actor accessing an OASIS node and OASIS node implementation details. Additionally, Sandia National Laboratories made one Additional Finding recommending the establishment of metrics to analyze how the implementation of the WEQ OASIS Suite of Business Practice Standards increases the usability, security, and reliability of conducting transactions through OASIS nodes.

As part of the Assessment Report of the NAESB Business Operations Practices and Standards, Sandia National Laboratories identified two potential Security Issues. The first vulnerability, classified has High level severity, addressed references to communication protocols that could be vulnerable to cyber-attacks. The second vulnerability, classified as Low level severity, addressed references to legacy or deprecated functionality. Additionally, Sandia National Laboratories made eight Additional Findings recommending the establishment of metrics to analyze how the implementation of the standards increase the reliability and security of electronic data exchanged between trading partners as well as practices that could prevent or increase the difficulty of a successful cyber-attack or exploitation by an adversary.

As part of the Addendum Report: Threat-based Examination of NAESB Standards and Business Operations, Sandia National Laboratories identified ten Additional Findings. These Additional Findings address best practices to mitigate or protect against specific cyber-attacks, considerations regarding standards development for emerging digital technologies, and recommendations for collaboration with government agencies or other standard development organizations.

NAESB would like to recognize the efforts of the working group of the Sandia National Laboratories Information Design Assurance Red Team (IDART) that prepared the surety assessment: Benjamin Anderson, Joshua Daley, Ryan Kao, and Marshall Riley. Additionally, NAESB would like to thank the subject matter experts that contributed their time and knowledge to assisting the Sandia National Laboratories IDART working group:

 Jim Buccigross, 8760, Inc.

 Lancen LaChance, GMO GlobalSign, Inc.

 Paul Sorenson, Open Access Technology International, Inc.

 Leigh Spangler, Latitude Technologies, LLC

**III. NAESB Response**

In anticipation of completion of the surety assessment, NAESB included on its 2019 Annual Plans a review of the final reports on the assessment and the development and/or modifications of standards or model business practices as needed to address any resulting recommendations from Sandia National Laboratories. Prior to delivery of the final reports, the U.S. DoE requested that, where possible, NAESB expediate resulting standards development efforts to address any identified potential Security Issues. To meet this goal, the Board Critical Infrastructure Committee volunteered to review the final reports and provide context for standards development to address the Security Issues and Additional Findings identified by Sandia National Laboratories.

After Sandia National Laboratories provided the final reports on the surety assessment in July 2019, the Board Critical Infrastructure Committee held two meetings in swift succession on August 7 and August 14. The committee reviewed each of the four reports and discussed how to address the potential Security Issues and Additional Findings. For the six potential Security Issues, the Board Critical Infrastructure Committee identified standard development activities to be considered by subcommittees within the RMQ, WEQ, and WGQ. For the Additional Findings, the Board Critical Infrastructure Committee identified twenty-two activities for NAESB to undertake. Of the Additional Findings, the Board Critical Infrastructure Committee identified seventeen that could be addressed through standards development. The remaining five Additional Findings were identified by the Board Critical Infrastructure Committee as areas not currently addressed by NAESB and needing further discussion and a determination on how to proceed by the NAESB Board of Directors.

NAESB is pleased to report that all standard development efforts to address recommendations made by Sandia National Laboratories to mitigate the six potential Security Issues as well as several standard development efforts to address the Additional Findings have been completed. The modifications resulting from the finalized standards development activities have been or will soon be incorporated into new publications of the RMQ Model Business Practices, the WEQ Business Practice Standards, and the WGQ Business Practice Standards. These standard development efforts modified the WGQ and RMQ EDM and IET Business Practice Standards/Model Business Practices, the NAESB Accreditation Requirements for Authorized Certification Authorities, the WEQ-001 OASIS Business Practice Standards, and the WEQ-002 OASIS Standards and Communication Protocols Business Practice Standards. In accordance with the recommendations from Sandia National Laboratories, these modifications seek to align security requirements with industry cybersecurity best practices, remove legacy functionality that could potentially provide a vehicle for cyber-attacks, and incorporate more secure communication protocols and encryption methodologies. Each specific modification is discussed in detail in Appendices A and B of this report.

Within the WEQ, standard development efforts were assigned to the WEQ Cybersecurity Subcommittee and WEQ OASIS Subcommittee, with several items jointly assigned to both subcommittees. The WEQ Cybersecurity Subcommittee was individually assigned standard development efforts to address the recommendations to mitigate the two potential Security Issues identified in the Assessment Report of the NAESB Public Key Infrastructure Program as well as seven standard development efforts to address Additional Findings found within that report, the Assessment Report of the NAESB Business Operations Practices and Standards, and the Addendum Report: Threat-based Examination of NAESB Standards and Business Operations. Related to the mitigation of the two potential Security Issues identified in the Assessment Report of the NAESB OASIS Standards, standard development efforts were individually assigned to the WEQ OASIS Subcommittee and jointly to the WEQ Cybersecurity Subcommittee and WEQ OASIS Subcommittee. The subcommittees were also jointly assigned standard development efforts to address one Additional Finding in the Addendum Report: Threat-based Examination of NAESB Standards and Business Operations.

Within the RMQ and WGQ, all standard development efforts were jointly assigned to the WGQ EDM Subcommittee and RMQ Information Requirements and Technical Electronic Implementation Subcommittee (IR/TEIS). These assigned activities included standard development efforts to address the recommendations to mitigate the two potential Security Issues identified in the Assessment Report of the NAESB Business Operations Practices and Standards as well as nine Additional Findings across the Assessment Report of the NAESB Business Operations Practices and Standards and the Addendum Report: Threat-based Examination of NAESB Standards and Business Operations.

Now that the standard development efforts to address the six potential Security Issues have been completed, the subcommittees are expected to reconvene as necessary to address the assigned standard development efforts regarding the remaining Additional Findings. NAESB also will continue to engage in discussions to determine how the organization should address the Additional Findings that propose activities in areas not currently addressed by the NAESB Business Practice Standards or Model Business Practices.

NAESB would like to recognize the efforts of the WEQ Cybersecurity Subcommittee, WEQ OASIS Subcommittee, WGQ EDM Subcommittee, and RMQ IR/TEIS for their leadership throughout the standard development processes:

 Rob Arbitelle, WEQ OASIS Subcommittee Co-Chair

Jim Buccigross, WEQ Cybersecurity Subcommittee Chair

 Mary Do, RMQ IR/TEIS Chair

 Ken Quimby, WEQ OASIS Subcommittee Co-Chair

 Matt Schingle, WEQ OASIS Subcommittee Co-Chair

 Leigh Spangler, WGQ EDM Chair

 Mike Steigerwald, WEQ OASIS Subcommittee Co-Chair

 JT Wood, WEQ OASIS Subcommittee Co-Chair

**IV. Conclusion**

The recommendations and considerations provided through the sponsorship of the DoE by Sandia National Laboratories as part of the surety assessment have provided NAESB with an invaluable resource to ensure that NAESB Business Practice Standards and Model Business Practices address the cybersecurity needs of the wholesale and retail gas and electric markets and will continue to do so. NAESB looks forward to continuing to work with the DoE and Sandia National Laboratories on future endeavors to meet the cybersecurity needs and other interests of the energy markets.

**Appendices A. Security Assessment Recommendations to Mitigate Security Issues and NAESB Responses**

*Detailed description of applicable Sandia National Laboratories findings, analyses, and recommendations and resulting NAESB standards development*

 **B. Surety Assessment Additional Findings for NAESB Consideration and NAESB Responses**

*Detailed description of applicable Sandia National Laboratories additional findings and resulting NAESB response*

**Appendix A – Surety Assessment Recommendations to Mitigate Security Issues and NAESB Responses**

Sandia National Laboratories identified six potential Security Issues within the NAESB Public Key Infrastructure Program, specifically the NAESB Accreditation Requirements for Authorized Certification Authorities, the WEQ OASIS Suite of Business Practice Standards, and the WGQ and RMQ IET and EDM Business Practice Standards/Model Business Practices. The finding, analysis, and recommendation to mitigate the potential security issue identified from Sandia National Laboratories as well as the standard development response by NAESB are described below.

*Assessment Report of the North American Energy Standards Board Public Key Infrastructure Program*

1. **Section 6.1.1 – Discrepancy between NAESB Standards and Certification Practices**

Language differences between the NAESB standards and CPS allow for a window of time where the CPS does not match the NAESB requirements and could result in non-compliant certificate operations.

**Level of Severity:** Low

**Sandia Analysis:** The GlobalSign and OATI CPS’s include NAESB specific language that is drawn from various NAESB standards. For example, the GlobalSign CPS includes text regarding the NAESB Authentication Requirements; and the OATI CPS includes text regarding cases where a certificate can be revoked. However, Section 1.5.4 *CPS Approval* Procedures of the GlobalSign CPS indicates the CPS will be updated on an “as needed” basis; and Section 2.3 *Certification Practice Statement Management* of the OATI CPS indicates it will be reviewed “at least annually and updated as necessary to reflect changes to applicable industry standards.”

**Sandia Recommendation:** 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.

**NAESB Response:** This Sandia recommendation was assigned to the WEQ Cybersecurity Subcommittee for review. In analyzing the recommendation, the subcommittee found that the NAESB Accreditation Requirements for Authorized Certification Authorities requires certificate authorities to utilize the most recent version of other industry standards referenced in the document. To add further clarity, the subcommittee recommended revisions to Section 1.1. to specify that the NAESB Accreditation Requirements for Authorized Certification Authorities contains the minimum technical and management details that must be met.

2. **Section 6.1.2 – Possible Incomplete Enforcement of NAESB Standards Assurance Levels**

CPS stated audit log retention periods do not enforce full coverage of all assurance levels as dictated by the NAESB standards.

**Level of Severity:** Low

**Sandia Analysis:** The GlobalSign CPS indicates that they retain audit logs for a period of “at least 10 years” (Section 5.4.3 *Retention Period for Audit Log*). This length of time meets the NAESB requirements for “Rudimentary”, “Basic”, and “Medium” assurance levels found in Section 4.5.2 of the *NAESB Accreditation Requirements for Authorized Certification Authorities*; however, the retention period for the “High” assurance level is given as 20 years. Since NAESB tools only requires a certificate at the “Basic” assurance level, it is unclear if “High” assurance level certificates have been issued.

**Sandia Recommendation:** 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”.)

**NAESB Response:** This recommendation was assigned to the WEQ Cybersecurity Subcommittee for review. In analyzing the recommendation, the subcommittee determined that the “High” assurance level should remain part of the NAESB Accreditation Requirements for Authorized Certification Authorities should the need for such an assurance level arise in the future. In the instance the “High” assurance level is utilized, the WEQ Cybersecurity will review the accompanying retention period to determine if modifications are needed. As part of discussions on this recommendation, GlobalSign indicated that its certificate practice statement (CPS) had been revised to address the issue raised by Sandia.

No modifications were proposed to address this recommendation.

*Assessment Report of the North American Energy Standards Board OASIS Standards*

3. **Section 6.1.1 – Significant Amounts of Sensitive Information Are Posted on OASIS**

Given the type and amount of information that is posted on OASIS, it is possible that a malicious actor could access a node using normal business practices or a cyber attack.

**Level of Severity:** Low

**Sandia Analysis:** Given the independent nature of OASIS Nodes, and the unique implementation details of each node, it is possible that an adversary could conduct a successful cyber attack to obtain the sensitive information located on that node. Alternatively, an adversary could follow legitimate practices to establish themselves as a participant or observer in OASIS and access the information in that manner.

However, FERC requires information such as transmission models, systems planning or facility studies, transfer capacity, and interconnections to be made available to enable business decision making and service requests. The assessment team believes this is all sensitive information that must be stored on the various OASIS Nodes.

The assessment team recognizes the difficulty of required posting of information that is deemed to be publicly available without requiring user registration and those fields must be supported by HTTP. This information contains information that is identifying by name and location which can be leveraged by an adversary. This elevates the need to keep encryption and securing of valid transactions consistent with the latest standards.

**Sandia Recommendation:** Continue to leverage the NAESB OASIS Subcommittee to ensure there is a balance between protecting sensitive information and meeting industry needs. In addition, the assessment team recommends that NAESB work with their partners and FERC to determine if more stringent security testing – similar to that used for ACAs – is desirable for OASIS Node operators to ensure the nodes are secure from cyber attacks. 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. 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 assessment team does feel the need to explicitly call out the potential for historical information regarding areas of constraint, interconnect/generation location information, and ownership of generation capacity to be used by an adversary in planning a cyber or physical attack against critical components of the grid. This information could be used to plan attacks that target critical interconnects or generation stations that would result in the greatest impact to grid operations. The team recommends that the OASIS Subcommittee consider the sensitivity of historical information and determine what information can be removed on a quarterly basis; however, outside of this consideration, the assessment team does not have any specific recommendations for actions that need to be taken. The assessment team review of the existing backup and recovery procedures did not reveal specific updates, the requirements are at an appropriate level for standards development.

**NAESB Response:** This recommendation was assigned jointly to the WEQ Cybersecurity Subcommittee and WEQ OASIS Subcommittee for review. In addressing the recommendation, the subcommittees were directed to review all standards within the WEQ OASIS Suite of Business Practice Standards (WEQ-001, WEQ-002, WEQ-003, and WEQ-013) and revise the standards as determined necessary (1) to replace and update references to SSL/TLS, (2) to align requirements for authentication and passwords with recommended best practices found in NIST SP 800-63B, and (3) to ensure data retention requirements are meeting recommended guidelines.

To replace and update the SSL/TLS references, the subcommittees reviewed all the WEQ OASIS Suite of Business Practice Standards and struck all references to SSL throughout the standards. Additionally, the subcommittees modified WEQ-002-2.3(d) to require the use of TLS Version 1.2 or higher and WEQ-002-5 to require the use of cryptographic security models conforming to FIPS Security Requirements for Cryptographic Modules FIPS-140-3 (which was released on March 22, 2019 and superseded FIPS-140-2).

To align requirements for authentication and passwords with NIST SP 800-63B, the subcommittees specifically reviewed WEQ-002-5.1 and WEQ-002-5 which establish the security and implementation/maintenance requirements for OASIS nodes. The subcommittees modified WEQ-002-5 to require that OASIS node providers apply industry best practices in implementing and maintaining OASIS nodes and supporting infrastructure. The standard now includes a reference to NIST SP 800-63B as the best practice guidelines for password and authentication requirements.

To ensure data retention requirements meet recommended guidelines, the WEQ OASIS Subcommittee reviewed all the WEQ OASIS Suite of Business Practice Standards to identify any data retention requirements. The subcommittee confirmed that all data retention periods specified in the standards are consistent with FERC regulations regarding posting and audit requirements found in 18 CFR 37.6 and 18 CFR 37.7.

The WEQ OASIS Subcommittee will continue to work in response to FERC directives as well as part of annual plan items and industry submitted standard requests to revise the WEQ OASIS Suite of Business Practice Standards as necessary. The Board Strategy Committee is also discussing how NAESB could be responsive to recommendations that the industry consider additional security testing for OASIS node operators.

4. **Section 6.1.2 – Implementation Details for OASIS Nodes Unspecified**

NAESB standards enumerate the requirements of OASIS nodes, but do not prescribe the manner in which a node implements the requirements. This allows the operators of each node to select the operating system, software, libraries, and other technical details of the system that provide the required functionality.

**Severity Level:** Low

**Sandia Analysis:** Since each node is implemented in an independent manner, it is possible that there are insecure system configurations that may provide an attack vector to an adversary. Compromising an OASIS node could allow an attacker to monitor communications, delete critical information, or cause an outage affecting the bidding process.

**Sandia Recommendation:** 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.

**NAESB Response:** This recommendation was assigned jointly to the WEQ Cybersecurity Subcommittee and WEQ OASIS Subcommittee for review. In addressing the recommendation, the subcommittees were directed to review all standards within the WEQ OASIS Suite of Business Practice Standards (WEQ-001, WEQ-002, WEQ-003, and WEQ-013) and revise the standards as determined necessary to (1) replace and update references to HTTP with HTTPS, (2) ensure web applications are secure against common vulnerabilities such as the OWASP Top 10, (3) require business continuity and disaster recovery exercises, and (4) require software patches and updates be implemented in a timely manner.

To replace and update references to HTTP with HTTPS, the subcommittees reviewed all of the WEQ OASIS Suite of Business Practice Standards and modified the standards to require all access to OASIS nodes utilize HTTPS protocols. Further, the subcommittees modified WEQ-002-2.3(d) to require the use of server-side HTTPS on the publicly available OASIS node homepage.

To address the remaining standard development efforts, the subcommittees modified WEQ-002-5 to require providers apply industry best practices in implementing and maintaining OASIS nodes and supporting infrastructure. In addition to the requirement discussed above, the standard now requires (1) the incorporation of firewalls, intrusion detection, and intrusion prevention systems, (2) the securing of OASIS applications against common vulnerabilities such as OWASP Top 10, (3) the application of security patches and updates in a timely manner, ideally within seven days, (4) performance of vulnerability scans quarterly and penetration testing annually, and (5) an annual review of OASIS node implementation to incorporate needed changes based on updates to industry recognized best practices.

In addition to the modifications to the WEQ OASIS Suite of Business Practice Standards described above, the WEQ Cybersecurity Subcommittee also modified Sections 5.1.1, 5.1.2, 5.1.6, 5.1.7, 5.2.1, and 5.2.7 of the NAESB Accreditation Requirements for Authorized Certification Authorities to reference the latest version of the FIPS Security Requirements for Cryptographic Modules (FIPS 140-3).

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

5. **Section 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).

**Severity Level:** High

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

**Sandia 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[[5]](#footnote-5). 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. 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.

**NAESB Response:** This recommendation was assigned jointly to the WGQ EDM Subcommittee and RMQ IR/TEIS. In addressing the recommendation, the subcommittees were directed to review the entirety of the WGQ and RMQ IET and EDM Business Practice Standards/Model Business Practices and revise the standards as determined necessary to (1) consider a requirement to implement fixes and patches for known vulnerabilities within 30 days of publication, (2) provide notice to trading partners of any systems or software that are not updated, (3) recommend an implementation window for major security bulletins or recommendations, and (4) review and replace references to SSL with TLS.

To address the first three standard development considerations, the subcommittees reviewed the entirety of the WGQ and RMQ IET and EDM Business Practice Standards/Model Business Practices. The standards and model business practices were modified to require trading partners to (1) evaluate software updates/patches within 30 days of release and implement as soon as reasonably practicable if a security risk is identified, (2) notify other trading partners of vulnerabilities that cannot be addressed and impact the security or integrity of data transmission, and (3) implement controls to proactively evaluate hardware and software to identify risk, detect malicious activity, and log information for forensic analysis. Additionally, the modifications clarify that the use of the standards/model business practices should be mutually agreed between trading partners unless security standards in the current/applicable version of the standards are not compatible with security standards in previous versions and/or specified otherwise by an applicable regulatory authority. Specifically, WGQ Standard Nos. 4.1.5, 4.1.39, 4.4.15, 4.1.39, 10.1.7, and 10.1.9 were reserved and replaced with new WGQ Standard Nos. 4.3.z1, 4.3.z2, 10.3.z1, and 10.3.z2. Additionally, WGQ EDM Business Practice Standards Appendices B and D were modified. RMQ Model Business Practice Nos. 7.1.9 was revised and 7.1.7 was reserved and replaced with 7.3.28.

To replace and update references to SSL with TLS, the subcommittees reviewed the entirety of the WGQ and RMQ IET and EDM Business Practice Standards/Model Business Practices. The standards and model business practices were modified to eliminate references to SSL and specify the use of TLS Version 1.2. Additionally, references within the standards to TLS were centralized to increase usability of the standards and better enable future revisions. Specifically, WGQ Standard Nos. 4.3.61, 4.3.83, 10.2.33, and 10.3.25 were modified as well as generally applicable language within the WGQ IET and EDM Business Practice Standards and the WGQ EDM Business Practice Standards Appendices B and D. WGQ Standard Nos. 4.3.61 and 4.3.83 were reserved. RMQ Model Business Practices No. 5.3.22, 5.3.4.14, 7.3.15, and 7.3.25 were modified as well as generally applicable language within the RMQ IET Model Business Practices.

6. **Section 6.1.2 – NAESB Standards Need Review for Unused or Unnecessary Functionality**

NAESB standards contain legacy or deprecated functionality.

**Severity Level:** Low

**Sandia 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.

**Sandia 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 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.

**NAESB Response:** This recommendation was assigned jointly to the WGQ EDM Subcommittee and RMQ IR/TEIS. The WGQ EDM Subcommittee, as part of a recurring annual plan item, is charged with reviewing and updating the technical characteristics contained in the appendices of the WGQ EDM Business Practice Standards. The WGQ EDM Business Practice Standards already require entities to update to the latest version of a protocol within 9 months of such version becoming generally available. The subcommittees were asked to consider adding similar requirements to the RMQ Model Business Practice Standards.

As part of the recurring annual plan item for the WGQ, revisions were made to the appendices of the WGQ EDM Business Practice Standards to update HTTP references and security and encryption requirements to conform with standard changes as well as to remove legacy protocols and allowable Transmission Control Protocol (TCP) ports.

Related to the RMQ Model Business Practices, the subcommittees revised Model Business Practice No. 7.1.9 to clarify that the use and upgrade or adoption of later versions of the model business practice standards should be mutually agreed upon unless specified otherwise by the applicable regulatory authority.

**Appendix B – Surety Assessment Additional Findings for NAESB Consideration and NAESB Responses**

Based on the final reports on the surety assessment provided by Sandia National Laboratories, the Board Critical Infrastructure Committee identified twenty-two Additional Findings. These findings are additional considerations or recommendations made by Sandia National Laboratories that do not address the six potential Security Issues.

*Assessment Report of the North American Energy Standards Board Public Key Infrastructure Program*

 1. **Section 4 – Metrics of Importance**

**Sandia Finding:** Metrics should be collected and analyzed to measure how the implementation of the PKI program increases the security and reliability of electronic data exchanges between trading partners. The following are some examples of metrics related to the PKI program that could be collected for NAESB and industry partners:

* Measure overall ACA activity including the number of new or renewed certificates issued, number of rejected requests, number of certificate revocations, and number of security anomalies[[6]](#footnote-6)
* Measure the best, median, average, and worst time it takes for an organization to detect, report, notify trading partners and the ACA about a compromised certificate
* Measure the best, median, average, and worst time for an updated revocation list to be issued for a compromised certificate
* Measure an organization’s level of compliance with updated revocation lists (i.e. – Are they checking for an updated revocation list with each transaction, or are they using some other time period)
* Measure the number of certificate compromises per organization
* Time for an ACA to issue a new certificate if the previous certificate was compromised

For the ACA metrics, NAESB could incorporate these statistics into required reporting during the annual ACA recertification process. For other organizations, these statistics could be self-reported – either to NAESB or maintained on a statistics webpage. If desired, NAESB could collect and tabulate the totals annually 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, or determining if NAESB standards need to be upgraded or revised.

**NAESB Response:** This is not currently a requirement of the NAESB Business Practice Standards/Model Business Practices nor is this a function currently provided by NAESB. The finding is being reviewed by the Board Strategy Committee as part of discussions identified by the Board Critical Infrastructure Committee as needing action or direction by the Board of Directors to determine how to proceed.

2. **Section 6.3 – Review of X.509 Security**

**Sandia Finding:** 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.

**NAESB Response:** This finding was assigned to the WEQ Cybersecurity Subcommittee for review. The WEQ Cybersecurity Subcommittee has a recurring annual plan item to review the WEQ-012 Public Key Infrastructure Business Practice Standards and the NAESB Accreditation Requirements for Authorized Certification Authorities and make modifications as necessary to address any vulnerabilities impacting Public Key Infrastructure. The subcommittee has now incorporated a review of the NIST NVD, ICS-CERT, US-CERT, and SANS Common Weaknesses Enumerated as part of this recurring effort. In evaluating these documents as part of the review in 2019, the subcommittee did not identify any vulnerabilities that needed to be addressed through modifications to the WEQ-012 Public Key Infrastructure Business Practice Standard or the NAESB Accreditation Requirements for Authorized Certification Authorities.

3. **Section 6.2 – Review of X.509 Security**

**Sandia Finding:** 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.

**NAESB Response:** This finding was assigned to the WEQ Cybersecurity Subcommittee for review. The subcommittee agreed with the finding from Sandia National Laboratories but determined not to make any modifications at this time as the NAESB Accreditation Requirements for Authorized Certification Authorities already specifies that the most current versions of applicable protocols are to be used.

*Assessment Report of the North American Energy Standards Board OASIS Standards*

 4. **Section 4 – Metrics of Importance**

**Sandia Finding:** Metrics should be collected and analyzed to measure how the implementation of the OASIS Standards increases the usability, security and reliability of conducting transactions through OASIS Nodes.

The following are some examples of metrics that could be collected for NAESB and industry partners to review and analyze:

* Measure the total number of OASIS users, and the number of OASIS observers
* Collect the type and version of web browsers used to access OASIS
* Enumerate the encryption methods used by the browsers to access OASIS information and note any requests for downgrading encryption to any type that does not meet security requirements (including encryption type “NONE”)
* Collect information on what pages and documents are accessed by various accounts
* Count the number of users that have an individual account, and the number of users that use a shared “entity” account
* Measure the number of daily transactions between business partners, and the number of transactions that fail or have errors that need to be corrected
* Measure the overall dollar amount of transactions completed each month
* Measure the best, median, average, and worst time for a transaction to be completed
* Using IP Geolocation, identify the number of logins that are completed from an unexpected geographic region
* Log the time of a user login, the average time they remain logged in, and the number of actions (pages/documents accessed, etc.) during the session

The various OASIS Nodes could maintain this information and submit the information to NAESB monthly to allow this information to be tabulated and shared with participating organizations. If necessary, data could be anonymized while still allowing organizations to rate their own performance against the industry norms.

This data could then be used in life-cycle decisions, identifying security anomalies, identifying poor security practices at an organization, or determining if NAESB standards need to be upgraded or revised to address any issues discovered.

**NAESB Response:** This is not currently a requirement of the NAESB Business Practice Standards/Model Business Practices nor is this a function currently provided by NAESB. The finding is being reviewed by the Board Strategy Committee as part of discussions identified by the Board Critical Infrastructure Committee as needing action or direction by the Board of Directors to determine how to proceed.

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

 5. **Section 4 – Metrics**

**Sandia Finding:** 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.

**NAESB Response:** This is not currently a requirement of the NAESB Business Practice Standards/Model Business Practices nor is this a function currently provided by NAESB. The finding is being reviewed by the Board Strategy Committee as part of discussions identified by the Board Critical Infrastructure Committee as needing action or direction by the Board of Directors to determine how to proceed.

6. **Section 6.1.4 – Use of Human Controls and Review in Operations**

**Sandia Finding:** 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.[[7]](#footnote-7) 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.

**NAESB Response:** This finding was assigned jointly to the WGQ EDM Subcommittee and RMQ IR/TEIS to consider standard(s) to address recommended guidelines for configuration and logging, network traffic monitoring, and alerting systems as well as standard(s) requiring manual continuity of operations in the event of abnormal behavior or failure conditions with the system. The WEQ Cybersecurity Subcommittee was also asked to investigate applicability of this finding to the WEQ Business Practice Standards.

The WGQ EDM Subcommittee and RMQ IR/TEIS modified the standards and model business practices to include both specific and broad adoption of system security measures as well as specific notifications and coordination during outages with effected trading partners. These changes were incorporated as part of the new WGQ Standard Nos. 4.3.z2 and 10.3.z2 and new RMQ Model Business Practice No. 7.3.28.

The WEQ Cybersecurity Subcommittee is in the process of scheduling a series of meetings to begin addressing the applicability of this finding to the WEQ Business Practice Standards.

7. **Section 6.1.5 – Separation of Business and Control Computer Networks**

**Sandia Finding:** 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.

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 [[8]](#footnote-8)

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

**NAESB Response:** This is not currently a requirement of the NAESB Business Practice Standards/Model Business Practices nor is this a function currently provided by NAESB. The finding is being reviewed by the Board Strategy Committee as part of discussions identified by the Board Critical Infrastructure Committee as needing action or direction by the Board of Directors to determine how to proceed.

8. **Section 6.1.6 – Continued Use of Different Security Paradigms**

**Sandia Finding:** 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.

**NAESB Response:** This finding was assigned jointly to the WGQ EDM Subcommittee and RMQ IR/TEIS Subcommittee and individually to the WEQ Cybersecurity Subcommittee. In addressing the finding, the subcommittees were asked to review the standards for legacy support references and remove those legacy items as recommended by Sandia National Laboratories.

The WGQ EDM Subcommittee and RMQ IR/TEIS modified the standards and model business practices to remove references to legacy references to software and communication protocols, specifically outdated versions of the PGP Protocol. The subcommittees modified WGQ Standard Nos. 10.2.34 and 10.3.15 as well as generally appliable language and appendices within the WGQ IET Business Practice Standards and added new WGQ Standard No. 10.2.z1. The subcommittees modified RMQ Model Business Practice No. 10.2.34 as well as generally applicable language and appendices within the RMQ IET Model Business Practices and added new Model Business Practice No. 10.2.39t.

The WEQ Cybersecurity Subcommittee modified the NAESB Accreditation Requirements for Certification Authorities to remove legacy functionality within Section 5.1.6.

9. **Section 6.1.6 – Continued Use of Different Security Paradigms**

**Sandia Finding:** 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.

**NAESB Response:** This finding was jointly assigned to the WGQ EDM Subcommittee and RMQ IR/TEIS. The item was addressed as part of the response to potential Security Issue 5.

To replace and update references to SSL with TLS, the subcommittees reviewed the entirety of the WGQ and RMQ IET and EDM Business Practice Standards/Model Business Practices. The standards and model business practices were modified to eliminate references to SSL and specify the use of TLS Version 1.2. Additionally, references within the standards to TLS were centralized to increase usability of the standards and better enable future revisions. Specifically, WGQ Standard Nos. 4.3.61, 4.3.83, 10.2.33, and 10.3.25 were modified as well as generally applicable language within the WGQ IET and EDM Business Practice Standards and the WGQ EDM Business Practice Standards Appendices B and D. WGQ Standard Nos. 4.3.61 and 4.3.83 were reserved. RMQ Model Business Practices No. 5.3.22, 5.3.4.14, 7.3.15, and 7.3.25 were modified as well as generally applicable language within the RMQ IET Model Business Practices.

10. **Section 6.1.6 – Continued Use of Different Security Paradigms**

**Sandia Finding:** An HTTPS[[9]](#footnote-9) 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[[10]](#footnote-10). 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.

**NAESB Response:** This finding as jointly assigned to the WGQ EDM Subcommittee and RMQ IR/TEIS. To address the finding, the subcommittees were asked to review the WGQ/RMQ EDM and IET Business Practice Standards/Model Business Practices to identify references to HTTP and replace with HTTPS as needed. The subcommittees were also instructed to consider the development of standards securing communications via certificates as recommended by Sandia National Laboratories.

The subcommittees reviewed the entirety of the WGQ/RMQ EDM and IET Business Practice Standards/Model Business Practices to identify references to HTTP and modified the standards/model business practices to specify the use of HTTPS whenever secure communications were required. The subcommittees modified WGQ Standard Nos. 4.3.60, 4.3.84, 10.3.4, and 10.3.16 as well as generally applicable language found in the WGQ EDM and IET Business Practice Standards. The subcommittees modified RMQ Model Business Practice Nos. 7.3.4 and 7.3.16 as well as generally applicable language in the RMQ IET Model Business Practices.

11. **Section 6.1.6 – Continued Use of Different Security Paradigms**

**Sandia Finding:** Key lengths must be updated to reflect current acceptable encryption strength[[11]](#footnote-11). 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[[12]](#footnote-12).

**NAESB Response:** This finding was assigned to the WEQ Cybersecurity Subcommittee and jointly to the WGQ EDM Subcommittee and RMQ IR/TEIS. To address the finding, the subcommittees were asked to review the standards and revise as necessary encryption requirements.

The WEQ Cybersecurity Subcommittee modified Section 5.1.6 of the NAESB Accreditation Requirements for Certification Authorities to update key lengths and encryption methods to align with the most current industry guidelines and best practices as identified by Sandia National Laboratories.

The WGQ EDM Subcommittee and RMQ IR/TEIS modified the standards and model business practices to meet current industry guidelines regarding key lengths and encryption methods, including updating references to a new version of PGP. WGQ Standard No. 4.3.83 was modified as well as generally applicable language in the WGQ EDM and IET Business Practice Standards. Generally applicable language within the RMQ IET Model Business Practices was modified as well.

12. **Section 6.1.6 – Continued Use of Different Security Paradigms**

**Sandia Finding:** Finally, IET business process as currently implemented may be vulnerable to both replay[[13]](#footnote-13) and amplification[[14]](#footnote-14) 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.

**NAESB Response:** This finding was assigned to the WEQ Cybersecurity Subcommittee and jointly to the WGQ EDM Subcommittee and RMQ IR/TEIS. In initially reviewing the assigned efforts, the priority of the subcommittees was to address items to mitigate security issues or otherwise easily addressed through standards development. The subcommittees are in the process of scheduling a series of meetings to address this finding. The WEQ Cybersecurity Subcommittee will consider this item as part of 2020 WEQ Annual Plan Item 6. The WGQ EDM Subcommittee will consider this item as part of 2020 WGQ Annual Plan Item 6. The RMQ IR/TEIS will consider this item as part of 2020 RMQ Annual Plan Item 6.

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

 13. **Section 2.3.1 – EDI Cyber Attack**

**Sandia Finding**: To better understand the impact this kind of outage has on business operations and operating costs, the team has identified several metrics that could be used to help quantify the impact of these kinds of events:

* Measure the number of daily transactions during normal operations and the number of daily transactions when using COOP procedures.
* Measure the number of hours worked by staff during normal operations and during COOP procedures. This should also include any time spent on recovering local systems or testing to ensure functionality of remote systems has been restored.
* Measure any additional expenses incurred due to utilizing COOP procedures. For example, if food must be provided due to staff working additional hours; or expenses due to overtime wages.
* Measure the number of errors made in transactions during normal operations, and the number of errors made when using COOP procedures.
* Measure the time the outage began, to the time full service is restored.
* Measure the time and expense to perform a forensic analysis of affected systems to determine the root cause of the attack or failure.
* Count the number of organizations affected by the outage.

Following a major outage, these metrics could be reported to NAESB to tabulate the total cost and impact of the event. This data could then be used in life-cycle decisions, vendor selection, analysis of continuity of operations/disaster recovery planning, and to determine if NAESB standards needed to be upgraded or revised.

**NAESB Response:** This is not currently a requirement of the NAESB Business Practice Standards/Model Business Practices nor is this a function currently provided by NAESB. The finding is being reviewed by the Board Strategy Committee as part of discussions identified by the Board Critical Infrastructure Committee as needing action or direction by the Board of Directors to determine how to proceed.

14. **Section 2.3.1 – EDI Cyber Attack**

**Sandia Finding:** The assessment team recommends that NAESB work through their existing relationships with TSA and NERC to develop more-detailed guidance on cyber security plans (including incident response procedures). An important recommendation is to ensure that NAESB members receive relevant cyber attack incident reporting. In addition to NAESB partner organizations above there exists a large resource of existing federal organizations with capability and responsibility to help in cyber security attacks against critical infrastructure. *Appendix C describes those organizations, their roles and responsibilities, capabilities and contact mechanisms*.

These recommendations are not intended to be used as a guide for compliance, or to replace current reporting that is required by the FERC or other federal or state regulatory agencies as this is outside the scope of the assessment.

**NAESB Response:** This is not currently a requirement of the NAESB Business Practice Standards/Model Business Practices nor is this a function currently provided by NAESB. The finding is being reviewed by the Board Strategy Committee as part of discussions identified by the Board Critical Infrastructure Committee as needing action or direction by the Board of Directors to determine how to proceed.

15. **Section 2.3.1 – EDI Cyber Attack**

**Sandia Finding:** Another part of the TSA/NERC engagement, would be to consider initiating development of incident report templates relevant to their stakeholders. Such a template, although likely voluntary, would ensure reporting is more complete and the standardization could include examples to help socialize the needs and improve relationships…

These reports can take the shape of a wizard driven reporting mechanism that populates a database such as the US CERT[[15]](#footnote-15), DHS[[16]](#footnote-16) and DOE[[17]](#footnote-17) incident report portals or develop your own document using guidance from NIST Computer Security Incident Handling Guide.

These recommendations are not intended to be used as a guide for compliance, or to replace current reporting that is required by the FERC or other federal or state regulatory agencies as this is outside the scope of the assessment.

**NAESB Response:** This is not currently a requirement of the NAESB Business Practice Standards/Model Business Practices nor is this a function currently provided by NAESB. The finding is being reviewed by the Board Strategy Committee as part of discussions identified by the Board Critical Infrastructure Committee as needing action or direction by the Board of Directors to determine how to proceed.

16. **Section 2.3.2 – Ukrainian Power Grid Attack**

**Sandia Finding:** 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.

**NAESB Response:** NAESB has confirmed that the applicable WEQ Business Practice Standards related to accessing OASIS nodes (WEQ-002-3.1(b)), participating in electronic tagging communications (WEQ-004-2.3), and accessing the NAESB Electric Industry Registry (WEQ-022-1.2) require the use of a digital certificate issued by a NAESB ACA on an individual basis.

The WEQ Cybersecurity Subcommittee has reviewed WEQ-012-1.9 which addresses the issuance of a digital certificate by a NAESB ACA and confirmed that for the applications described in the WEQ Business Practice Standards, it is appropriate for a NAESB ACA to issue a digital certificate for an individual subscriber, a specific role, a device, and a software application.

The WGQ EDM Subcommittee and RMQ IR/TEIS were asked to review the current authentication methods identified within the WGQ Business Practice Standards and RMQ Model Business Practices and consider employing two-factor authentication on an individual user level for secure websites. The subcommittees agreed that secure websites should utilize individual user credentials and modified the standards to comport with this finding. However, the general consensus was to not deploy two-factor authentication at this time as it was determined that the current process for authenticating individuals through the use of a user identification/password maintains the security of websites without complicating the login process, especially for users that access multiple websites. The subcommittees modified WGQ Standards Nos. 4.3.60, 4.3.84, 10.3.4, and 10.3.16 as well as generally applicable language within the WGQ EDM and IET Business Practice Standards. The subcommittees modified generally applicable language within the RMQ IET Model Business Practices.

17. **Section 2.3.2 – Ukrainian Power Grid Attacks**

**Sandia Finding:** A relatively static communications environment, such as the NAESB-responsible systems, should definitely be considered for whitelisting. However, how whitelisting is implemented will be a hardware-specific implementation and thus outside NAESB standards scope. In consideration of the whitelisting ROI are several factors:

* Some related information must be made publicly available and this must not be blocked by the whitelisting implementation.
* Since NAESB standards do not specify the environment there could be negative impacts to non-EDI applications which are hosted on the same servers.

The whitelisting decision must consider the support environment. The point being that if a legitimate transaction is blocked by the whitelisting, how quickly could the error be corrected given coverage and capability of the support team?

**NAESB Response:** This finding was assigned jointly to the WGQ EDM Subcommittee and RMQ IR/TEIS. In initially reviewing the assigned efforts, the priority of the subcommittees was to address items to mitigate security issues or otherwise easily addressed through standards development. The subcommittees are in the process of scheduling a series of meetings to address this finding. The WGQ EDM Subcommittee will consider this item as part of 2020 WGQ Annual Plan Item 6. The RMQ IR/TEIS will consider this item as part of 2020 RMQ Annual Plan Item 6.

18. **Section 3.1 – Trends in Operation**

**Sandia Finding:** As technology is integrated into the control systems, it is important to ensure that abnormal events can be detected and that abnormal conditions do not prevent operations from being conducted or, after an outage, from being restored. To ensure that problems can be detected, the assessment team recommends that existing metering be used to verify information being provided by the control systems and, in the event that the computer system and the metering system disagree, that response personnel can be deployed to investigate in a timely manner. However, to ensure that response personnel are able to manually restore proper functioning, the assessment team notes it is imperative that the responders have a method to disconnect the equipment from the control network and conduct manual operations until normal operations can be restored.

**NAESB Response:** This is not currently a requirement of the NAESB Business Practice Standards/Model Business Practices nor is this a function currently provided by NAESB. The finding is being reviewed by the Board Strategy Committee as part of discussions identified by the Board Critical Infrastructure Committee as needing action or direction by the Board of Directors to determine how to proceed.

19. **Section 3.2 – Government and Industry Standards**

**Sandia Finding:** To address the security of the various emerging technologies such as those listed above, the assessment team recommends that organizations utilize the government and industry standards that are relevant to the technologies deployed. For example, NIST provides a number of whitepapers and standards related to cloud computing. These standards can be found at the NIST Cloud Computing Related Publications page and include special publications from the 500 and 800 series, and a variety of NIST cloud computing research papers.[[18]](#footnote-18) Some of the documents referenced on this page are:

* NIST SP 500-299: NIST Cloud Computing Security Reference Architecture (Draft)
* NIST SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing, December 2011
* NIST SP 800-145: NIST Definition of Cloud Computing, September 2011
* NIST SP 800-146: Cloud Computing Synopsis and Recommendations, May 2012

NIST also maintains a page related to the Internet of Things (IoT) that includes reports related to trust, fog computing (cloud computing for IoT), and other areas related to the IoT.[[19]](#footnote-19)

Other resources provided by NIST that address the above technologies include:

* NIST 800-124rev1: Guidelines for Managing the Security of Mobile Devices in the Enterprise[[20]](#footnote-20)
* NISTIR 8144 (DRAFT): Assessing Threats to Mobile Devices and Infrastructure - The Mobile Threat Catalog[[21]](#footnote-21)
* NCCoE Project: Mobile Device Security: Cloud and Hybrid Builds[[22]](#footnote-22)

**NAESB Response:** This finding was reviewed by the Board Digital Committee and incorporated into the committee’s inaugural report to the NAESB Board of Directors. The report prepared by the Board Digital Committee describes the digital transformation taking place within the energy industry and is intended to aid NAESB as the organization considers new standard activities to support digital technologies.

20. **Section 3.3 – Emerging Technologies**

**Sandia Finding:** Data Analytics – this is an area of massive lab capability and investment. With respect to traditional internet communications analysis and detection the lab helps develop and implement novel defenses for both government and military networks. This effort includes advanced analysis for emerging threats and attack techniques. Sandia leads the national laboratory modeling and simulation in the development of a suite of network emulation and analysis capabilities collectively referred to as Emulytics™ (a holistic approach to system emulation and analytics)[[23]](#footnote-23). Over the last decade, we have developed and deployed a suite of cyber emulation, modeling, and analysis tools that support uses including predictive simulation, training, test & evaluation, and resilient system design.

Emulytics™ experiments provide safe and isolated environments to study and test computing and communications systems and to exercise and train cyber staff. Enterprise computing and control systems environments are well supported today and we are developing support for emerging mobile computing and Internet of Things environments. Emulytics environments scale well and can be deployed on systems as small as a laptop and on clusters with hundreds of high performance servers. Our methodologies support the application of the scientific method to the study of cyber systems, and our tools make it easier to design, deploy, and collect data from virtualized experiments rapidly, reliably, and repeatedly.

Machine Learning – a method of data analysis that automates analytical model building. It is a branch of artificial intelligence based on the idea that systems can learn from data, identify patterns and make decisions with minimal human intervention. Machine learning was the focus of a recently completed grand challenge laboratory directed research and development effort.[[24]](#footnote-24)

Behavior Analytics – a tool that reveals the actions users take within a digital product. It organizes raw event data such as clicks into a timeline of each user's behavior, also known as a user journey. At Sandia, researchers model both malware and attacker behaviors to identify malicious activity. For example, Sandia scientists used virtual machine (VM) technology and a supercomputing cluster to watch how botnets work and explore ways to stop them.[[25]](#footnote-25)

Software Defined Networking (SDN) – approach to network management that enables dynamic, programmatically efficient network configuration in order to improve network performance and monitoring making it more like cloud computing than traditional network management. SDN was recently adapted into a Sandia patented alternative reality which can be deployed as a network defense. The capability is knows as HADES (High-fidelity Adaptive Deception & Emulation System) and it feeds a hacker not what he needs to know but what he wants to believe. HADES won a 2017 R&D 100 Award presented annually by R&D Magazine.

Zero Trust Networks[[26]](#footnote-26) – Zero trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter. No single specific technology is associated with zero trust; it is a holistic approach to network security that incorporates several different principles and technologies.

Fileless Malware[[27]](#footnote-27) - Fileless malware refers to a cyberattack technique that uses existing software, allowed applications, and authorized protocols to carry out malicious activities. Fileless malware sneaks in without using traditional executable files as a first level of attack like traditional malware. Rather than using malicious software or downloads of executable files as its primary entry point onto corporate networks, fileless malware often hides in memory or other difficult-to-detect locations. From there, it is written directly to RAM rather than to disk to execute a series of events or is coupled with other attack vectors such as ransomware to accomplish its malicious intent. And because fileless malware doesn’t write anything to disk like traditional malware does, it is much harder to detect and may defeat traditional security systems.

**NAESB Response:** This finding was reviewed by the Board Digital Committee and incorporated into the committee’s inaugural report to the NAESB Board of Directors. The report prepared by the Board Digital Committee describes the digital transformation taking place within the energy industry and is intended to aid NAESB as the organization considers new standard activities to support digital technologies.

21. **Section 3.4 – Recommended Future Assessments**

**Sandia Finding:** 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[[28]](#footnote-28): “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.”

**NAESB Response:** This finding was assigned jointly to the WEQ Cybersecurity Subcommittee and WEQ OASIS Subcommittee. In addressing the finding, the subcommittees were asked to consider the development of standard(s) recommending best practices or requiring internal/external scans of nodes and a security assessment/penetration test as outlined by Sandia National Laboratories.

The subcommittees addressed this finding in conjunction with standards development to address Security Issue 4. As discussed above, the subcommittees modified WEQ-002-5 to require that OASIS node providers apply industry best practices in implementing and maintaining OASIS nodes and supporting infrastructure. Included as part of these modifications are requirements to perform vulnerability scans and penetration testing of OASIS applications on a quarterly basis and conduct business continuity and disaster recovery exercises annually.

22. Section 3.4 – Recommended Future Assessments

**Sandia Finding:** 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.

**NAESB Response:** This finding was assigned jointly to the WGQ EDM Subcommittee and the RMQ IR/TEIS. In addressing the finding, the subcommittees were asked to review the WGQ and RMQ EDM and IET Business Practice Standards/Model Business Practices to determine if additional language should be added to recommend customers and software vendors work together.

The subcommittees addressed this finding by modifying generally applicable language within the WGQ EDM and IET Business Practice Standards to encourage security assessments and coordination between customers, vendors, and trading partners. There was general consensus that this Additional Finding was not applicable to the RMQ Model Business Practices.

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 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-5)
6. A security anomaly would be anything unusual enough, or serious enough, to be noted. For example, a known criminal organization attempting to obtain a certificate. [↑](#footnote-ref-6)
7. NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS) <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf> [↑](#footnote-ref-7)
8. (<https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf>) [↑](#footnote-ref-8)
9. *Securing the Web*, retrieved on June 10, 2019, from <https://www.w3.org/2001/tag/doc/web-https> [↑](#footnote-ref-9)
10. RFC 2617: *HTTP Authentication: Basic and Digest Access Authentication*, retrieved on June 10, 2019, from <https://tools.ietf.org/html/rfc2617> [↑](#footnote-ref-10)
11. 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-11)
12. Symantec Corporation. *PGP Command Line 9.0 User’s Guide*. Symantec, 2006. [↑](#footnote-ref-12)
13. *Replay Attacks*, retrieved on June 10, 2019, from <https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/replay-attacks> [↑](#footnote-ref-13)
14. *DNS Amplification Attacks*, retrieved on June 10, 2019, from <https://www.us-cert.gov/ncas/alerts/TA13-088A> [↑](#footnote-ref-14)
15. US-CERT Incident Reporting System, <https://www.us-cert.gov/forms/report> [↑](#footnote-ref-15)
16. Report Cyber Incidents, <https://www.dhs.gov/how-do-i/report-cyber-incidents> [↑](#footnote-ref-16)
17. DOE - JC3 Incident Reporting, <https://tickets.ijc3.doe.gov> [↑](#footnote-ref-17)
18. <https://www.nist.gov/itl/nist-cloud-computing-related-publications> [↑](#footnote-ref-18)
19. <https://www.nist.gov/topics/internet-things-iot> [↑](#footnote-ref-19)
20. <https://csrc.nist.gov/publications/detail/sp/800-124/rev-1/final> [↑](#footnote-ref-20)
21. <https://www.nccoe.nist.gov/sites/default/files/library/mtc-nistir-8144-draft.pdf> [↑](#footnote-ref-21)
22. <https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/cloud-hybrid> [↑](#footnote-ref-22)
23. <https://www.sandia.gov/emulytics/> [↑](#footnote-ref-23)
24. <https://www.sandia.gov/news/publications/lab_accomplishments/articles/2018/adv_science_and_tech.html> [↑](#footnote-ref-24)
25. <https://www.sandia.gov/news/publications/lab_accomplishments/_assets/documents/lab_accomplish-2010.pdf> [↑](#footnote-ref-25)
26. <https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/> [↑](#footnote-ref-26)
27. <https://www.carbonblack.com/resources/definitions/what-is-fileless-malware/> [↑](#footnote-ref-27)
28. <https://www.sans.org/security-resources/policies/application-security/pdf/web-application-security-policy> [↑](#footnote-ref-28)