Assessment Report of the North American Energy Standards Board Open Access Same-Time Information Systems (OASIS) Standards

16 July ***2019***

Prepared for the Department of Energy and

North American Energy Standards Board

Prepared By

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

Acknowledgements

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

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

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

Ryan Kao, IDART Analyst
Sandia National Laboratories
Autonomous Cyber Systems

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

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

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

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

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

This page intentionally left blank.

Table of Contents

Executive Summary

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

This report provides an analysis of the Open Access Same-Time Information Systems (OASIS) standards and guides developed by NAESB. The assessment team used the Information Design Assurance Red Team (IDART™) methodology to conduct the analysis and assessment of the OASIS standards and associated documents.[1]

This assessment was executed by the Information Design Assurance Red Team (IDART™) due to information that was provided to the team at an on-site meeting held in August 2017. Given the importance of the OASIS standards, this assessment was added to the overall effort at the request of program manager, Mr. Christopher Freitas, of the Department of Energy (DOE), Office of Fossil Energy, Office of Oil and Natural Gas. The intent is to provide a surety assessment of the OASIS standards and guides to ensure the secure implementation of OASIS nodes and secure business operation.

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

The analysis showed that the NAESB OASIS Standards provide reasonable surety that the OASIS Nodes, and the business operations conducted on them are operating in a secure manner, and that only authorized organizations or individuals may access the sensitive information stored on the nodes. The only vulnerabilities identified by the assessment team were related to sensitive information that is required by FERC to be present, and the independent implementations of the OASIS Nodes which could result in the use of insecure configurations. Specifically, the team identified the following:

- Significant amounts of sensitive information is stored on OASIS Nodes, but these are required by FERC and industry needs
- Implementation details for OASIS Nodes are left up to individual organizations, which may result in insecure configurations

Overall, the assessment team found that the NAESB OASIS Standards provide a solid foundation to ensure that information located on OASIS Nodes, and the transactions performed in OASIS can be conducted in a reliable and secure manner. However, the team does recommend that NAESB work with their partners and FERC to determine if more stringent security testing of OASIS Nodes is desirable; and to consider when historical information can be removed from the system. The team also noted that there are multiple strengths from other NAESB activities – such as maintaining the OASIS Subcommittee – that provide additional surety to the OASIS system.

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

1 Introduction

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

This report provides an analysis of the Open Access Same-Time Information Systems (OASIS) standards and guides developed by NAESB. The assessment team used the Information Design Assurance Red Team (IDART™) methodology to conduct the analysis and assessment of the OASIS standards and associated documents.[2]

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

This assessment was executed by the Information Design Assurance Red Team (IDART™) due to information that was provided to the team at an on-site meeting held in August 2017. Given the importance of the OASIS standards, this assessment was added to the overall effort at the request of program manager, Mr. Christopher Freitas, of the Department of Energy (DOE), Office of Fossil Energy, Office of Oil and Natural Gas. The intent is to provide a surety assessment of the OASIS standards and guides to ensure the secure implementation of OASIS nodes and secure business operation.

This task involved a review of the following NAESB documents:

- WEQ-001 NAESB Open Access Same-Time Information Systems (OASIS) Business Practice Standards, Version 2.1
- WEQ-002 NAESB Open Access Same-Time Information Systems Business Practice Standards and Communication Protocol (S&CP), Version 2.1
- WEQ-003 NAESB Open Access Same-Time Information Systems (OASIS) Data Dictionary Business Practice Standards, Version 2.1
- WEQ-013 NAESB Open Access Same-Time Information Systems (OASIS) Implementation Guide Business Practice Standards, Version 2.1

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

2 Objective and Purpose of the NAESB OASIS Standards

The Energy Policy Act of 1992 and FERC Orders 888 and 889 required transmission providers and other participants in the electricity market to develop a method to openly conduct business to ensure the proper operation of the power grid. This resulted in the creation of the Open-Access Same-Time Information Systems (OASIS) as the mechanism to allow these operations.

The NAESB OASIS business practice, technical standards, data dictionary, and implementation guide:

- Define specific transaction and processing requirements
- Establish technical standards for OASIS
- Established Data Element specifications
- Provides guidance for processing specific types of business transactions
- Includes templates used, and actions that may be taken, to execute a transaction on OASIS

Combined, these specifications define processes, procedures, and technical details that allow transmission providers and other participants in the electricity market to provide or obtain services in accordance with FERC requirements.

3 Critical Success Factors

Factors which are critical to the success of the NAESB OASIS Standards were identified during the analysis of the documents listed in Section 1. These factors are crucial in determining if the NAESB Standards are providing a reasonable level of surety when conducting transactions through OASIS. Critical success factors identified include the following:

- The majority of the requirements in the OASIS Standards are followed, with only a small percentage being excluded due to the Transmission Provider's tariff not including the provision or through the use of a waiver.
- Participants use the definitions for data elements that are provided in the data dictionary and only valid values are accepted.
- OASIS Node operators provide fair connectivity and information to all users of that particular node. (i.e. – Traffic shaping or throttling is not used to provide some users a competitive advantage.)

4 Metrics of Importance

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.

5 Surety Assessment Research

Research of the NAESB OASIS Standards began at the on-site meeting that was held at NAESB facilities in Houston on August 3, 2017. From that meeting, the following documents were identified as critical to an analysis of the OASIS Standards:

- WEQ-001 Open Access Same-Time Information Systems (OASIS)
- WEQ-002 OASIS Standards and Communication Protocols
- WEQ-003 OASIS Data Dictionary
- WEQ-013 OASIS Implementation Guide

In addition to these standards, the assessment team reviewed other available information related to OASIS, including user guides, how-to’s, references, and other documentation provided by OASIS Node providers.

From a high-level view, the assessment team found two areas of concern related to OASIS. The first area is the amount of sensitive information that is posted on OASIS. This is a relatively minor concern since there is a NAESB OASIS Subcommittee that engages in constant discussions with their members and FERC to ensure there is a balance between providing this information and meeting industry needs. The second area of concern is that NAESB (by design) has not provided requirements related to the implementation details of required functionality. This allows OASIS Node providers to meet NAESB requirements with insecure or obsolete technologies. A more detailed discussion on this second area can be found in the following section.

6 Surety Assessment Analysis and Recommendations

This analysis focused on the operation of OASIS Nodes, and the standards and business practices used to conduct business between transmission providers and other participants in the electricity market. The assessment team recommends that NAESB conduct an internal analysis to determine if more stringent security testing – similar to that used for ACAs – is desirable for OASIS Node operators.

6.1 Security Issues

Items listed in this section deal specifically with vulnerabilities that could provide an opportunity to an attacker to conduct malicious activities that would affect the availability or security of OASIS Nodes, compromise the sensitive information stored on those nodes, or interrupt business transactions conducted using OASIS.

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

6.1.1 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: LOW

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.

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[3]

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.

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.

Level: LOW

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

[3] NIST 800-52 section 3.1 Protocol Version Support https://csrc.nist.gov/CSRC/media/Publications/sp/800-52/rev-2/draft/documents/sp800-52r2-draft2.pdf

OASIS node could allow an attacker to monitor communications, delete critical information, or cause an outage affecting the bidding process.

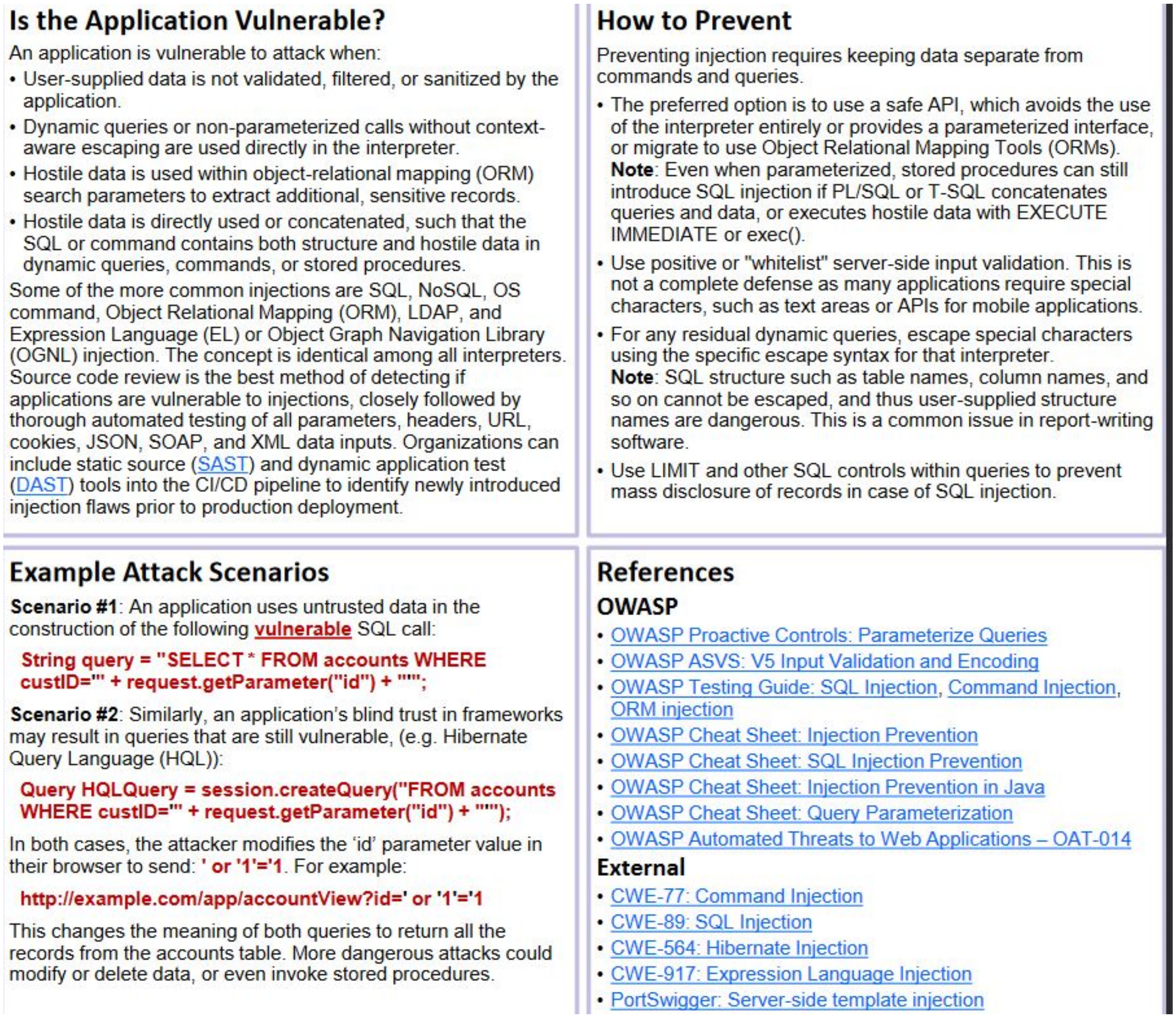
Recommendation: To mitigate this issue, the assessment team recommends that all OASIS nodes follow industry best practices to secure their systems. This would include, but is not limited to:

- Ensuring web applications are secure against common vulnerabilities such as the OWASP Top 10[4] OWASP addresses common vectors for attack, and methods for prevention for each identified security risk.
- Encrypting all communications (as allowable) using an encryption module that is validated against FIPS 140-2[5,6] . The assessment team recommends removal of HTTP communication for status notifications and utilizing either HTTPS solutions or utilize encrypted email notification. In section WEQ-002-5.1 appears to require encrypted communication but in WEQ-002-4.2 allowances are made for HTTP notifications. NIST SP 800-131A REV 2 provides guidance for acceptable encryption (AES 128 bit or better), random bit generation, hash functions and message authentication codes.
- Utilizing the latest versions of all critical standards (such as TLS) to ensure all possible vulnerabilities are addressed
- Verifying and validating all external inputs
- Conducting business continuity and disaster recovery exercises on an annual basis
- Applying patches and updates in a timely manner; ideally no longer than 7 days after the patch or update becomes available (if practical). It is imperative that implementation details, system configurations, and software dependencies be considered prior to applying updates as some updates can have a detrimental impact on functionality. Any of these items that have an impact on the update process must be tracked and communicated to dependent parties.

[4] https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

[5] FIPS 140-2: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

[6] Validated encryption modules: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules



Is the Application Vulnerable?

An application is vulnerable to attack when:

- User-supplied data is not validated, filtered, or sanitized by the application.
- Dynamic queries or non-parameterized calls without context-aware escaping are used directly in the interpreter.
- Hostile data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records.
- Hostile data is directly used or concatenated, such that the SQL or command contains both structure and hostile data in dynamic queries, commands, or stored procedures.

Some of the more common injections are SQL, NoSQL, OS command, Object Relational Mapping (ORM), LDAP, and Expression Language (EL) or Object Graph Navigation Library (OGNL) injection. The concept is identical among all interpreters. Source code review is the best method of detecting if applications are vulnerable to injections, closely followed by thorough automated testing of all parameters, headers, URL, cookies, JSON, SOAP, and XML data inputs. Organizations can include static source (SAST) and dynamic application test (DAST) tools into the CI/CD pipeline to identify newly introduced injection flaws prior to production deployment.

How to Prevent

Preventing injection requires keeping data separate from commands and queries.

- The preferred option is to use a safe API, which avoids the use of the interpreter entirely or provides a parameterized interface, or migrate to use Object Relational Mapping Tools (ORMs). **Note**: Even when parameterized, stored procedures can still introduce SQL injection if PL/SQL or T-SQL concatenates queries and data, or executes hostile data with EXECUTE IMMEDIATE or exec().
- Use positive or "whitelist" server-side input validation. This is not a complete defense as many applications require special characters, such as text areas or APIs for mobile applications.
- For any residual dynamic queries, escape special characters using the specific escape syntax for that interpreter. **Note**: SQL structure such as table names, column names, and so on cannot be escaped, and thus user-supplied structure names are dangerous. This is a common issue in report-writing software.
- Use LIMIT and other SQL controls within queries to prevent mass disclosure of records in case of SQL injection.

Example Attack Scenarios

Scenario #1: An application uses untrusted data in the construction of the following **vulnerable** SQL call:

```
String query = "SELECT * FROM accounts WHERE
custID='" + request.getParameter("id") + "'";
```

Scenario #2: Similarly, an application's blind trust in frameworks may result in queries that are still vulnerable, (e.g. Hibernate Query Language (HQL)):

```
Query HQLQuery = session.createQuery("FROM accounts
WHERE custID='" + request.getParameter("id") + "'");
```

In both cases, the attacker modifies the 'id' parameter value in their browser to send: **' or '1'='1**. For example:

http://example.com/app/accountView?id=' or '1'='1

This changes the meaning of both queries to return all the records from the accounts table. More dangerous attacks could modify or delete data, or even invoke stored procedures.

References

OWASP

- OWASP Proactive Controls: Parameterize Queries
- OWASP ASVS: V5 Input Validation and Encoding
- OWASP Testing Guide: SQL Injection, Command Injection, ORM injection
- OWASP Cheat Sheet: Injection Prevention
- OWASP Cheat Sheet: SQL Injection Prevention
- OWASP Cheat Sheet: Injection Prevention in Java
- OWASP Cheat Sheet: Query Parameterization
- OWASP Automated Threats to Web Applications – OAT-014

External

- CWE-77: Command Injection
- CWE-89: SQL Injection
- CWE-564: Hibernate Injection
- CWE-917: Expression Language Injection
- PortSwigger: Server-side template injection

Figure 1 OWASP Document Layout

6.2 Strengths of the NAESB OASIS Standards

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

6.2.1 Constant Review by the OASIS Subcommittee

The OASIS subcommittee works closely with their partners and FERC to ensure that there is a balance between providing/protecting sensitive information in OASIS and meeting industry needs. This constant review allows for rapid identification of issues and ensures industry needs are considered when making decisions. As mentioned in Section 6.1.1 the assessment team does recommend they also consider when historical information can be removed from the system.

6.2.2 Development of a Comprehensive Data Dictionary

NAESB's WEQ-003 Data Dictionary provides comprehensive definitions for field formats, restrictions on the values, size constraints, and a definition for what data element is used for. This rigorous definition helps prevent some types of cyber attacks – such as buffer overflows – since the size and type of each field is predefined.

6.2.3 Strong Processes for Vetting New OASIS Accounts

To access OASIS, an organization or individual must:

1) Be registered in the Electric Industry Register (EIR)
2) Obtain a certificate from an ACA, which includes vetting of the organizational and personal information submitted to the ACA
3) Request an OASIS account

This process includes a number of checks at each step to ensure that an individual is properly identified and authenticated, and has a legitimate business reason for obtaining access.

7 Summary

The assessment team conducted an analysis of the NAESB OASIS Standards, which included the following documents:

- WEQ-001 NAESB Open Access Same-Time Information Systems (OASIS) Business Practice Standards, Version 2.1
- WEQ-002 NAESB Open Access Same-Time Information Systems Business Practice Standards and Communication Protocol (S&CP), Version 2.1
- WEQ-003 NAESB Open Access Same-Time Information Systems (OASIS) Data Dictionary Business Practice Standards, Version 2.1
- WEQ-013 NAESB Open Access Same-Time Information Systems (OASIS) Implementation Guide Business Practice Standards, Version 2.1

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

The analysis showed that the NAESB OASIS Standards provide reasonable surety that the OASIS Nodes, and the business operations conducted on them are operating in a secure manner, and that only authorized organizations or individuals may access the sensitive information stored on the nodes. The only vulnerabilities identified by the assessment team were related to sensitive information that is required by FERC to be present, and the independent implementations of the OASIS Nodes which could result in the use of insecure configurations.

The following strengths of the NAESB OASIS Standards were identified:

- Constant review by the NAESB OASIS Subcommittee ensures that only information required to meet industry needs is stored on OASIS Nodes

- NAESB OASIS Standards provide a comprehensive data dictionary, which rigorously defines the format and content of data fields
- Strong processes for vetting new OASIS accounts ensure only valid users are provided with login credentials

The following weaknesses in the security of the OASIS Nodes and business operations were identified:

- Significant amounts of sensitive information is stored on OASIS Nodes, but these are required by FERC and industry needs
- Implementation details for OASIS Nodes are left up to individual organizations, which may result in insecure configurations

Overall, the assessment team feels that these vulnerabilities are a minor concern since they are driven by federal regulations and industry needs. However, the assessment team would encourage NAESB to work with their partners and FERC to determine if more stringent security testing of OASIS Nodes is desirable; and to consider when historical information can be removed from the system.

8 Conclusion

This report is intended to contribute to the improve of NAESB OASIS Standards and identify any vulnerabilities that could pose a risk to OASIS Nodes and the business operations that use OASIS, and was developed with the best information available at the time of the assessment.

Overall, the assessment team found that the NAESB OASIS Standards provide a solid foundation to ensure that information located on OASIS Nodes, and the transactions performed in OASIS can be conducted in a reliable and secure manner. However, the team does recommend that NAESB work with their partners and FERC to determine if more stringent security testing of OASIS Nodes is desirable; and to consider when historical information can be removed from the system. The team also noted that there are multiple strengths from other NAESB activities – such as maintaining the OASIS Subcommittee – that provide additional surety to the OASIS system.

9 Appendix A: Abbreviations and Acronyms

ACA	Authorized Certificate Authority
CA	Certification Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DOE	Department of Energy
FE	Office of Fossil Energy
FERC	Federal Energy Regulatory Commission
IDART	Information Design Assurance Red Team
IETF	Internet Engineering Task Force
NAESB	North American Energy Standards Board
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
OASIS	Open Access Same-Time Information Systems
PKI	Public Key Infrastructure
RFC	Request for Comment
SNL	Sandia National Laboratories
WEQ	Wholesale Electric Quadrant

10 Appendix B: Relevant Document Summary Table

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

Relevant Source Document	Relevant Section	Location in This Report
N/A	N/A	N/A

The assessment team found that all of the OASIS documents reviewed were sufficient, and the team does not have any recommended updates for the documents reviewed for this report.