As part of the surety assessment, Sandia National Laboratories provided NAESB with the following reports: Public Key Infrastructure (PKI) Report, OASIS Standards Report, Business Operation Practices and Standards Report, and Addendum Report. Within these reports, Sandia National Laboratories identified six explicit recommendations for NAESB consideration:

1. PKI Report – Section 6.1.1 Discrepancy between NAESB Standards and Certification Practice Statements

**Sandia Finding:** 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

**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:**

1. PKI Report – Section 6.1.2 Possible Incomplete Enforcement of NAESB Standards Assurance Levels

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

**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:**

1. OASIS Standards Report – Section 6.1.1 Significant Amounts of Sensitive Information Are Posted on OASIS

**Sandia Finding:** 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.

**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. Therefore, the sensitive information must be stored on the various OASIS Nodes.

**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.

**NAESB Response:**

1. OASIS Standards Report – Section 6.1.2 Implementation Details for OASIS Nodes Unspecified

**Sandia Finding:** 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

**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
* Encrypting all communications (as allowable)
* Utilizing the latest versions of all critical standards (such as TLS)
* Verifying and validating all external inputs
* Conducting business continuity and disaster recovery exercises
* Applying patches and updates in a timely manner

**NAESB Response:**

1. Business Operations Practices and Standards Report – Section 6.1.1 NAESB Standards Refer to Vulnerable Versions of Communication Protocols

**Sandia Finding:** 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).

**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:** To ensure outdated protocols do not provide a vector for future attacks, the assessment team recommends replacing any reference to a specific version of a technology or protocol with a reference to indicate that the latest version of the technology or protocol should be used. If desirable, a time limit such as “within 30 days of publication” could be added to allow some time for organizations to update their systems and software. 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 even if a new standard is not yet available

**NAESB Response:**

1. Business Operations Practices and Standards Report – Section 6.1.2 NAESB Standards Need Review for Unused or Unnecessary Functionality

**Sandia Finding:** NAESB standards contain legacy or deprecated functionality

**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 some legacy or rarely used items – such as the “refnum” data field in the WGQ/REQ/RGQ Internet Electronic Transport Related Standards – that could prove to be an attack vector in the future.

**Sandia Recommendation:** To ensure legacy functionality does not provide a vector for future attacks, the assessment team recommends NAESB conduct occasional (ex. annual) reviews of their standards to determine if there is functionality that is defined, but unused, so it can be removed, deprecated or updated. This could be performed by having organizations report what functionality they are currently using, no longer using, or have never used. If utilization of functionality falls below a certain threshold or level of need it could be labeled for deprecation and removal.

**NAESB Response:**

Additionally, the Business Operations Practices and Standards Report and the Addendum Report identified practices or requirements that could prevent or increase the difficulty of a successful attack or exploitation by an adversary or recommended future actions:

1. Business Operations Practices and Standards Report – Section 6.2.1 Use of Human Control and Review in Operations

**Sandia Finding:** Currently, business and control operations are performed or authorized by an individual who is familiar with normal operations. For example, business operations for a specific trading partner is generally assigned to a specific individual who oversees all interactions with that partner. This allows the human to note abnormal behavior and communicate with the trading partner to determine if the operations are accurate. In addition, the control networks have human operators monitoring the state of the system and will take action to prevent damaging conditions from occurring. For example, a human will ensure that there is gas flowing in a pipeline if there is a risk of a vacuum condition.

With the current trend towards more automation and computer control, this strength should be considered when replacing human operators with autonomous systems.

**NAESB Response:**

1. Addendum Report – Section 4.2 Follow-on Assessment Activities

**Sandia Recommendation:** Since OASIS nodes are implemented independently, the team recommends conducting scans or penetration tests of the various nodes to identify any nodes that are using older software versions, leak information about the system (ex. list software versions being used), or have vulnerable implementations of their web applications. Since each node could be unique in its software, environment, and supporting security systems, the assessment

**NAESB Response:**

**Sandia Recommendation:** Perform security assessments on software that is used by large number of organizations to identify vulnerabilities that could be exploited by an attacker. The assessment team recommends that the software vendors, in partnership with their customers, determine the specifics of these assessments.

**NAESB Response:**