Draft Surety Assessment Findings Work Paper – Critical Infrastructure Committee Feedback

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 findings/analyses/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.

**Critical Infrastructure Committee Feedback:** Additional guidance has been requested from the NAESB ACAs.

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”.)

**Critical Infrastructure Committee Feedback:** Additional guidance has been requested from the NAESB ACAs.

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.

The assessment team does feel the need to explicitly call out the potential for historical information to assist an adversary in planning an attack. Information regarding areas of constraint, interconnect/generation location information, and ownership of generation capacity could be used to identify critical components of the grid. This information could be used to plan attacks that target these 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.

**Critical Infrastructure Committee Feedback:** The committee noted that additional clarity concerning this finding, analysis, and recommendation would aid in the identification of considerations for standards development; specifically, a data sensitivity analysis that would identify the specific data Sandia National Laboratories is referencing when stating that the NAESB OASIS Subcommittee should be leveraged to continue “to ensure there is a balance between protecting *sensitive information* and meeting industry needs.” It would be helpful if the data sensitivity analysis identified the specific data that may pose a cybersecurity risk should it be compromised.

Additionally, the committee noted Sandia National Laboratories recommends that OASIS node operators “ensure the nodes are secure from cyber attacks.” To assist in the identification of standards development to carry out this recommendation, the committee agreed it would be beneficial if the final report identified risk mitigation steps that could be incorporated into the standards to strengthen the security of the OASIS nodes as well as strategies for response recovery should a node be compromised.

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](https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf)
* Encrypting all communications (as allowable) using an encryption model that is validated against [FIPS 140-2](https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf) (Validated encryption modules: <https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules> )
* 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)

**Critical Infrastructure Committee Feedback:** The committee noted that additional clarity concerning this finding, analysis, and recommendation would aid in the identification of considerations for standards development.

Regarding the securing of web applications against common vulnerabilities, the committee noted that the identification of OWASP Top 10 is helpful but that it would be beneficial if Sandia National Laboratories could identify potential modifications to the standards for specific steps to mitigate those vulnerabilities.

The committee also noted the benefit of a final report that would identify which communications should be encrypted and would identify specific recommendations regarding best practices for encryption algorithms, including the method of encryption and relevant details on implementation such as key length.

Additionally, regarding the recommendation to utilize the latest version of all critical standards, the committee noted that it would be helpful if Sandia National Laboratories could identify the minimum acceptable versions of these standards and/or the versions of these standards that should no longer be utilized due to known cybersecurity risks.

Finally, the committee noted a need for additional information to further clarify potential modifications to the standards that should be considered as part of recommendations to verify and validate all external outputs.

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. 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.

There are a variety of reasons for not applying updates to existing systems, such as:

• Existing systems may not be compatible with updated software packages or protocol versions

• Updated software may be too expensive to integrate

• Other business-related reasons

Therefore, the assessment team recommends the organization that owns the system notify their trading partners of any systems or software that have not been updated within the 30-day window. This notification should include comments regarding any risks in utilizing the legacy system, and details regarding any mitigations that are in place. This allows business partners to assess the risk of conducting business over those systems.

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 the 30-day window, even if a new version of the standard is not yet available or finalized.

1. **Critical Infrastructure Committee Feedback:** The committee noted that additional clarity concerning this finding, analysis, and recommendation would aid in the identification of considerations for standards development. The committee reiterated the difficulties in the NAESB Business Practice Standards referencing the latest version of a technology or protocol instead of a specific version number. In recognition of this, the committee suggested of greater benefit to NAESB would be the identification of the minimum acceptable versions of SSL/TLS and/or the versions of SSL/TLS that that should no longer be utilized due to known cybersecurity risks.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 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 10% the functionality could be flagged as deprecated and removed from the standard at the following annual review. The assessment team also recommends including a mechanism where an organization can request that the deprecated functionality be retained in the standards.

**Critical Infrastructure Committee Feedback:** The committee noted that additional clarity concerning this finding, analysis, and recommendation would aid in the identification of considerations for standards development. The committee agreed that an annual review of functionality can be beneficial and noted that NAESB already undertakes yearly evaluations of the Quadrant Electronic Delivery Mechanism Related Standards Manual, the WEQ-012 Public Key Infrastructure Business Practice Standards, and the NAESB Accreditation Requirements for Authorized Certification Authorities. Additionally, the committee stated that entities can request modifications to the standards, including removal of deprecated functionality, through the NAESB Request for Standards Development Process. Beyond the “refnum” data field, the committee questioned as to if there were additional legacy or rarely used items in any of the standards or documentation included as part of the surety assessment that NAESB should evaluate.

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

1. PKI Report – Section 6.3 Review of X.509 Security

**Sandia Recommendation:** The assessment team recommends 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. 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.

**Critical Infrastructure Committee Feedback:** The committee noted that additional clarity concerning this finding, analysis, and recommendation would aid in the identification of considerations for standards development; specifically, any guidance as to databases or other industry reference documents NAESB should be considering as part of its annual evaluation of the WEQ-012 PKI Standards and NAESB Accreditation Requirements for Authorized Certification Authorities.

Additional guidance has been requested from the NAESB ACAs.

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. The assessment team recommends that, at a minimum, humans retain the ability to disengage any automated system and take manual control in the event of abnormal behavior or failure condition. In addition, operators should evaluate existing metering and sensors (pressure sensors, flow sensors, etc.) on a quarterly basis (or even daily for highly critical systems, if practical) to ensure that the automated/digital systems are reporting accurate information.

**Critical Infrastructure Feedback:** The committee noted that additional clarity concerning this finding would aid in the identification of considerations for standards development. The committee agreed that human verification can be helpful but noted the existence of monitoring technology to alert asset owners if a device begins to operate outside of normal parameters or if the health of a system fails. The committee questioned there are existing industry guidelines or best practices that could be considered for incorporation as references into the NAESB Business Practice Standards.

1. Business Operations Practices and Standards Report – Section 6.2.2 Separation of Business and Control Computer Networks

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

**Critical Infrastructure Committee Feedback:** The committee noted that additional clarity concerning this finding would aid in the identification of considerations for standards development. The committee agreed that the separation of control and business networks is a helpful recommendation already being utilized as an industry best practice and questioned if there are additional steps or modifications which should be reviewed for potential incorporation into the NAESB Business Practice Standards.

1. Business Operations Practices and Standards Report – Section 6.2.3 Continued Use of Different Security Paradigms

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

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

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

**Critical Infrastructure Committee Feedback:** The committee noted that additional clarity concerning this finding would aid in the identification of considerations for standards development; specifically, an analysis on the sufficiency of the current encryption algorithms, including the method of encryption and relevant details on implementation such as key length, contained in the standards and NAESB Accreditation Requirements for Authorized Certification Authorities. Additionally, the committee noted that, given the increased dependency between the gas and electric markets, an analysis comparing the use of different versus a singular security paradigm by the industries would be beneficial.

1. Addendum Report – Section 2.2.1 Adversary Models

**Sandia Finding:** There are a variety of adversary models that can be used to evaluate the capabilities of an adversary, each with their own strengths and weaknesses…([Defense Science Boards’ Taxonomy of Cyber Security Adversaries](https://apps.dtic.mil/dtic/tr/fulltext/u2/a569975.pdf), [Generic Threat Matrix – Sandia National Laboratories](https://idart.sandia.gov/_assets/documents/SAND2007-5791_Categorizing-Threat_Generic-Threat-Matrix.pdf), [Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector – Idaho National Laboratory](https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf), [Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats](https://www.energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf))

The assessment team prefers utilizing the Generic Threat Matrix since it provides generic profiles that can be used to characterize different levels of adversaries and their related capabilities; and makes it easier to reevaluate adversaries based on their changing capabilities. For example, when a new zero-day exploit is discovered, this allows a less capable adversary to act as a highly capable adversary – until the vulnerability used by the exploit is patched, or other mitigations can be put in place. By using this generic matrix, an organization can quickly decide if this temporary increase in capability will allow for identified attack vectors to be exploited.

However, the assessment team strongly encourages an organization to review the various threat models that have been defined by government agencies, industry groups, academia, and other organizations to determine what model will provide the most utility to their organization.

**Critical Infrastructure Committee Feedback:** The committee noted that additional clarity concerning this finding would aid in the identification of considerations for standards development. As identified by the committee, the Defense Science Boards’ Taxonomy of Cyber Security Adversaries is based on models from the Department of Defense. The committee suggested of greater benefit may be the use of an adversary model specifically applicable to the energy sector, such as the Idaho National Laboratory’s Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector or the SANS Institute’s Industrial Control System Cyber Kill Chain. Additionally, the committee noted the benefit of a final report that utilized an energy sector specific threat model to perform an assessment of the current standards and identify recommendations to mitigate any identified risks.

1. Addendum Report – Section 2.2.2 Attack Scenarios Against Current Operations

**Sandia Finding:** *An ACA issuing a certificate to a fictitious organization*: In this scenario, an attacker manages to convince an ACA to issue a certificate to a fictitious organization. It was indicated in the on-site meeting that, for someone to use this certificate to access OASIS, they would also need to be established in the EIR – which would require the attacker to have a level of presence suitable to make it through the various checks. (For example, it would actually have to be registered as a valid business with an appropriate Secretary of State or other official entity.) In addition, the organizational and individual authentication requirements for an ACA to issue a certificate are robust, and should prevent this from occurring.

**Critical Infrastructure Committee Feedback**: The committee noted that additional clarity concerning this finding would aid in the identification of considerations for standards development; specifically, the identification of the attack paths that led Sandia National Laboratories to include each scenario and recommendations for modifications to the standards to mitigate the risks for each attack path. For instance, the draft Addendum Report indicates that the identification of “several ways to perform denial of service attacks against the submission of a nomination (disrupt ISP service at either organization, a denial-of-service attack by flooding an organization with network traffic, corruption of the nomination information, etc)” led to the inclusion of the “Malicious Modification of Nominations” scenario.

1. Addendum Report – Section 2.2.2 Attack Scenarios Against Current Operations

**Sandia Finding:** *A pipeline could be stressed by over supply or over purchase of gas*: In this scenario, an organization (or an attacker able to impersonate the organization) nominates capacity or makes purchases that are outside appropriate bounds. In this scenario, it was indicated that the pipelines themselves would still deliver gas, but that there could be a commercial impact for upwards of three days. This scenario was mitigated since there are personal levels of involvement for each transaction. Specifically, that there is an individual who is managing the day-to-day transactions for each account, and that there is some level of personal relationship between organizations. Therefore, it was expected that large increases or decreases in nominated capacity would be noticed quickly, allowing human intervention before damage occurs.

**Critical Infrastructure Committee Feedback:** The committee noted that additional clarity concerning this finding would aid in the identification of considerations for standards development; specifically, the identification of the attack paths that led Sandia National Laboratories to include each scenario and recommendations for modifications to the standards to mitigate the risks for each attack path. For instance, the draft Addendum Report indicates that the identification of “several ways to perform denial of service attacks against the submission of a nomination (disrupt ISP service at either organization, a denial-of-service attack by flooding an organization with network traffic, corruption of the nomination information, etc)” led to the inclusion of the “Malicious Modification of Nominations” scenario.

1. Addendum Report – Section 2.2.2 Attack Scenarios Against Current Operations

**Sandia Finding:** *Nomination of, but failure to use, large quantity of capacity (and variations)*: From the discussion, it was expected that this scenario would be noticed within hours by the pipeline; or be noticed almost immediately by a shipper who had nominated capacity but had nothing flow. In addition, it was noted that the upstream and downstream confirmation process, and the other business processes in the background – such as billing – would make it difficult to manipulate the scheduled nomination for only a segment of the pipeline. It was also noted that, for wholesale gas, gas can only be delivered to the locations identified in the contract and cannot be diverted or redirected. In addition, excess/unused capacity can be easily sold on the spot market.

**Critical Infrastructure Committee Feedback:** The committee noted that additional clarity concerning this finding would aid in the identification of considerations for standards development; specifically, the identification of the attack paths that led Sandia National Laboratories to include each scenario and recommendations for modifications to the standards to mitigate the risks for each attack path. For instance, the draft Addendum Report indicates that the identification of “several ways to perform denial of service attacks against the submission of a nomination (disrupt ISP service at either organization, a denial-of-service attack by flooding an organization with network traffic, corruption of the nomination information, etc)” led to the inclusion of the “Malicious Modification of Nominations” scenario.

1. Addendum Report – Section 2.2.2 Attack Scenarios Against Current Operations

**Sandia Finding:** *Malicious modification of nominations*: This scenario can involve the modification of a nomination or a denial of service against the submission of a nomination. From the on-site discussion, it was determined that there are several business processes involved in nominating, scheduling, and billing that occur in each nomination period. In addition, it was indicated that these generally use different software packages and are monitored by a variety of individuals at an organization – essentially putting a human in the loop (or multiple humans) when it comes to the flow of gas. In addition, it was noted that the relationships between organizations are generally assigned to specific individuals, resulting in the individual being aware of normal business needs and requirements.

**Critical Infrastructure Committee Feedback:** The committee noted that additional clarity concerning this finding would aid in the identification of considerations for standards development; specifically, the identification of the attack paths that led Sandia National Laboratories to include each scenario and recommendations for modifications to the standards to mitigate the risks for each attack path. For instance, the draft Addendum Report indicates that the identification of “several ways to perform denial of service attacks against the submission of a nomination (disrupt ISP service at either organization, a denial-of-service attack by flooding an organization with network traffic, corruption of the nomination information, etc)” led to the inclusion of the “Malicious Modification of Nominations” scenario.

1. Addendum Report – Section 2.2.2 Attack Scenarios Against Current Operations

**Sandia Finding:** *An attacker able to steal an organization’s certificate/credentials for OASIS*: In this scenario, an attacker can obtain access to OASIS by impersonating an organization with legitimate access. During the discussion, it was noted that, since any action taken on OASIS is viewable by all parties, the organization that had their credentials stolen would be able to see any malicious activity done by the attacker impersonating them and be able to take remediation measures. (Such as communicating a compromise of their certificate to the ACA, trading partners, etc. and utilizing alternate channels to conduct business.)

**Critical Infrastructure Committee Feedback:** The committee noted that additional clarity concerning this finding would aid in the identification of considerations for standards development; specifically, the identification of the attack paths that led Sandia National Laboratories to include each scenario and recommendations for modifications to the standards to mitigate the risks for each attack path. For instance, the draft Addendum Report indicates that the identification of “several ways to perform denial of service attacks against the submission of a nomination (disrupt ISP service at either organization, a denial-of-service attack by flooding an organization with network traffic, corruption of the nomination information, etc)” led to the inclusion of the “Malicious Modification of Nominations” scenario.

1. Addendum Report – Section 2.2.2 Attack Scenarios Against Current Operations

**Sandia Finding:** *Compromise of an ACA*: In this scenario, a capable adversary – such as a nation-state – is able to compromise the certificate authority, bringing into question any certificates that they have issued. This scenario is of concern to the ACA themselves, and they take active measures to prevent this scenario. It was also noted that, in general, organizations have alternative contact information (phone, fax, etc.) for their partners, which would allow them to set up alternative mechanisms for conducting business.

**Critical Infrastructure Committee Feedback:** The committee noted that additional clarity concerning this finding would aid in the identification of considerations for standards development; specifically, the identification of the attack paths that led Sandia National Laboratories to include each scenario and recommendations for modifications to the standards to mitigate the risks for each attack path. For instance, the draft Addendum Report indicates that the identification of “several ways to perform denial of service attacks against the submission of a nomination (disrupt ISP service at either organization, a denial-of-service attack by flooding an organization with network traffic, corruption of the nomination information, etc)” led to the inclusion of the “Malicious Modification of Nominations” scenario.

1. Addendum Report – Section 2.2.2 Attack Scenarios Against Current Operations

**Sandia Finding:** *Backend system security*: It was noted in the on-site meeting that the industry has purposefully chosen to not address this through the NAESB standards.

**Critical Infrastructure Committee Feedback:** The committee noted that additional clarity concerning this finding would aid in the identification of considerations for standards development; specifically, the identification of the attack paths that led Sandia National Laboratories to include each scenario and recommendations for modifications to the standards to mitigate the risks for each attack path. For instance, the draft Addendum Report indicates that the identification of “several ways to perform denial of service attacks against the submission of a nomination (disrupt ISP service at either organization, a denial-of-service attack by flooding an organization with network traffic, corruption of the nomination information, etc)” led to the inclusion of the “Malicious Modification of Nominations” scenario.

1. Addendum Report – Section 2.3.1 EDI Cyber Attack

**Sandia Finding**: In April 2018, it was reported that a number of companies experienced a communication network failure due to a cyber attack targeting a third-party electronic data interchange (EDI) platform. It is reported that this platform is used by more than 100 organizations in the natural gas industry.

It needs to be noted that the Sandia assessment team has not conducted an analysis of the attack itself, and has not been provided any specific information related to the systems and networks impacted by the attack; therefore, the summary in this section was constructed from publicly available news sources. In addition, since the assessment team does not have detailed information on the attack, there are no specific recommendations regarding this event. If more information regarding this attack is desired, the assessment team recommends organizations contact the providers of the affected EDI platform…

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 need to be upgraded or revised.

Note: 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. However, the assessment team felt that they would provide this information as it would allow organizations, and their trading partners, to make business decisions related to their normal operations, creation of contingency plans, and development of their COOP.

**Critical Infrastructure Committee Feedback:** The committee agreed that incident reporting is helpful but that additional clarity concerning this finding would aid in the identification of considerations for standards development. The committee noted that much of the incident reporting information could be considered classified and should be kept confidential as it may be valuable to nefarious actors. The committee stated that there are existing information sharing networks and questioned if there are additional categories of information entities should be reporting and/or additional agencies or regulators that information should be made available to.

1. Addendum Report – Section 2.3.2 Ukrainian Power Grid Attack

**Sandia Finding:** In December 2015, it was reported that a cyberattack had resulted in Ukrainian power companies experiencing unscheduled power outages. These outages affected 30 substations and over 200,000 customers were without power for 1 to 6 hours.

Follow-on reporting indicated that malware – specifically the BlackEnergy malware – was found on the organizations’ networks and was used to gain access to the business network and, from there, allowed the attacker to use a VPN to access the companies’ control network. According to the Wired article “Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid” the attackers spent months performing reconnaissance of the business network and stealing credentials for the VPN that workers used to remotely log into the control network. (This VPN did not require two-factor authentication.) Once in the control network, the attacker crafted custom malware to attack communication components within that network to make recovery more difficult. In addition, to increase the difficulty of recovering, the attackers took the UPS systems for the control centers offline, and performed a Denial-of-service attack against the phone center, so the outages could not be reported and tracked. Finally, the attackers also used the KillDisk malware to delete key files in computer systems, preventing them from being operated. While power was restored after a few hours, it was also reported that even two months later the control centers were still not back to normal operations, and required workers to manually operate the breakers.

It should be noted that the initial attack vector was the use of a phishing email and a malicious Microsoft Word document that allowed the BlackEnergy malware to be installed.

A true air-gap between the business and control networks would have prevented the attacker from pivoting into the SCADA network and gaining control of the Human-machine Interface (HMI) systems that allowed them to control the breakers. If an organization requires a connected between these networks (or the SCADA network and the Internet) to exist – even for a brief period of time (ex. to download firmware updates) the connection should be restricted to only authorized traffic and individuals, it should use robust authentication methods such as two-factor authentication, whitelisting of IP addresses, and monitoring to ensure that only authorized operations are performed while the connection exists.

ICS-CERT issued an alert, “Cyber-Attack Against Ukrainian Critical Infrastructure” ([IR-ALERT-H-16-056-01](https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01)) regarding the incident, and this report provides a brief description of the event, and recommended mitigations. These mitigations discuss applying best practices across the entire business and operations space, which include: supply chain risk management, asset tracking, user tracking, system maintenance and updates, and “strategic technology refresh”. Of note is that they recommended contingency plans for continuity of operations and system shutdown. The full list of recommended mitigations and links to other resources, can be found in the ICS-CERT report. ICS-CERT also maintains a “[Recommended Practices](https://ics-cert.us-cert.gov/Recommended-Practices)” site that provides additional guidance on securing OT networks, including any connections to IT networks.

**Critical Infrastructure Committee Feedback:** The committee agreed with the finding regarding the the benefits of two-factor authentication and whitelisting but noted that additional clarity concerning this finding would aid in the identification of considerations for standards development; specifically, the identification of any areas currently within the standards that do not require two-factor authentication but should as well as the identification of any potential websites for which entities should whitelist IP addresses. Additionally, the committee noted the potential benefits of an analysis on the current two-factor authentication requirements as identified by the standards with recommendations for modifications to strengthen any identified weaknesses or vulnerabilities.

1. Addendum Report – Section 3.1 Trends in Operations

**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.

**Sandia Recommendation:** 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.

**Critical Infrastructure Committee Feedback:** The committee noted that the recommendation addresses control systems and noted that additional clarity concerning this finding and recommendation would aid in the identification of considerations for standards development; specifically, if there are recommendations that should be considered regarding business transactions or commercial communications or existing industry standards regarding meter verification that should be evaluated or considered as references.

1. Addendum Report – Section 3.1 Trends in Operations

**Sandia Finding:** One of the key trends in listed in Deloitte’s “[2019 Power and Utilities Industry Outlook](https://www2.deloitte.com/us/en/pages/energy-and-resources/articles/power-and-utilities-industry-outlook.html)” is the use of technology to improve operations. This includes adoption of smart-grid technologies including real-time information, and the “digitalization and integration of operational systems, back-office systems, and supply chain management.” However, as new technologies such as cloud computing, mobile device integration, and real-time communications are adopted, these create new cyber security challenges and could provide an adversary with an attack vector against utility companies.

**Sandia Recommendation:** To address the security of the various technologies 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](https://www.nist.gov/itl/nist-cloud-computing-related-publications). Some of the documents referenced on this page are:

* [NIST SP 500-299](http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Reference_Architecture_2013.05.15_v1.0.pdf): NIST Cloud Computing Security Reference Architecture (Draft)
* [NIST SP 800-144](http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf): Guidelines on Security and Privacy in Public Cloud Computing, December 2011
  + [NIST SP 800-145](http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf): NIST Definition of Cloud Computing, September 2011
  + [NIST SP 800-146](http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf): Cloud Computing Synopsis and Recommendations, May 2012

NIST also maintains a [page](https://www.nist.gov/topics/internet-things-iot) 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.

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

* [NIST 800-124rev1](https://csrc.nist.gov/publications/detail/sp/800-124/rev-1/final): Guidelines for Managing the Security of Mobile Devices in the Enterprise
* [NISTIR 8144 (DRAFT)](https://www.nccoe.nist.gov/sites/default/files/library/mtc-nistir-8144-draft.pdf): Assessing Threats to Mobile Devices and Infrastructure - The Mobile Threat Catalog
* [NCCoE Project](https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/cloud-hybrid): Mobile Device Security: Cloud and Hybrid Builds

**Critical Infrastructure Committee Feedback:** The committee agreed that the report provides helpful references regarding emerging technologies but noted that additional clarity concerning this finding and recommendation would aid in the identification of considerations for standards development; specifically, with the emergence of new technology trends such as mobile technology, could technology, and smart grid technology, if there are identified actions or areas of standards development NAESB should be evaluating to ensure that the standards continue to address secure communications across new platforms.

1. Addendum Report – Section 3.1 Trends in Operations

**Sandia Finding:** One of the key trends in listed in Deloitte’s “[2019 Power and Utilities Industry Outlook](https://www2.deloitte.com/us/en/pages/energy-and-resources/articles/power-and-utilities-industry-outlook.html)” is the use of technology to improve operations. This includes adoption of smart-grid technologies including real-time information, and the “digitalization and integration of operational systems, back-office systems, and supply chain management.” However, as new technologies such as cloud computing, mobile device integration, and real-time communications are adopted, these create new cyber security challenges and could provide an adversary with an attack vector against utility companies.

**Sandia Recommendation:** The assessment team recommends that, prior to the adoption and deployment of new technologies, organizations investigate what it takes to operate the systems in secure manner by reviewing resources provided by NIST, ICS-CERT, and other government organizations. (For example, DHS maintains a portal for their [cybersecurity resources](https://www.dhs.gov/science-and-technology/csd-resources).) This will ensure that operations can be properly secured prior to deployment of the new systems and technologies, ensuring new attack vectors are not introduced.

**Critical Infrastructure Committee Feedback:** As above, the committee agreed that the report provides helpful references regarding emerging technologies but noted that additional clarity concerning this finding and recommendation would aid in the identification of considerations for standards development; specifically, with the emergence of new technology trends such as mobile technology, could technology, and smart grid technology, if there are identified actions or areas of standards development NAESB should be evaluating to ensure that the standards continue to address secure communications across new platforms.

1. Addendum Report – Section 3.2 Recommended Future Assessments

**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 team recommends that the node owner perform these assessments on their own systems.

**Critical Infrastructure Committee Feedback:** The committee noted that additional clarity regarding this recommendation would aid in the identification of considerations for standards development; specifically, the identification of references, parameters, or timing considerations NAESB could evaluate.

1. Addendum Report – Section 3.2 Recommended Future Assessments

**Sandia Recommendation:** Perform security assessments on software, services or platforms (SPPs) that are used by more than 10% of organizations or carry more than 10% of total transactions as measured by volume or dollar value. This percentage can be adjusted based on operational needs and total number of SSPs that fall within this range. In addition, the assessment team recommends that this be performed on an annual basis, or anytime there is a major update to a specific SSP. The assessment team recommends that software vendors, in partnership with their customers, determine specifics of these assessments to ensure that all relevant risks are addressed.

**Critical Infrastructure Committee Feedback:** As above, the committee noted that additional clarity regarding this recommendation would aid in the identification of considerations for standards development; specifically, the identification of references or parameters NAESB could evaluate.