North American Energy Standards Board

801 Travis, Suite 1675, Houston, Texas 77002
Phone: (713) 356-0060, Fax: (713) 356-0067, E-mail: naesb@naesb.org
Home Page: www.naesb.org

To: Board Critical Infrastructure Committee

Re: Draft Surety Assessment from Sandia National Laboratories – Work Paper

To help facilitate discussion concerning the latest draft surety assessment from Sandia National Laboratory, this work paper was created at the direction of the Critical Infrastructure Committee Chair, Cade Burks and Vice Chair, Dave Darnell. The purpose of this work paper is to highlight areas needing additional information to support NAESB's future efforts to address the recommendations that will be contained in the 2018 Surety Assessment. Specifically, five areas for potential modifications have been identified by the Chair and Vice Chair of the committee.

1. The format and structure of the current draft surety assessment is different than that of the 2006 Surety Assessment. (Issue 1)
2. The level of detail in the specific findings in the draft 2018 Surety Assessment is not consistent with the findings in the 2006 Surety Assessment. (Issue 2)
3. The analysis provided in the draft 2018 Surety Assessment contains numerous statements and assumptions that do not have an easily identifiable supporting analysis. (Issue 3)
4. The draft 2018 Surety Assessment does not provide an adequate analysis on the potential types of cyber security attacks, including potential vulnerabilities, if any, within the standards and how to mitigate. (Issue 4)
5. The draft 2018 Surety Assessment does not include any discussion on potential impacts to reliability that may be caused by a commercial attack, as specifically requested by the Critical Infrastructure Committee. (Issue 5)

The specific items noted above are discussed in the below sections as noted:

1.) As stated in the past, the committee noted that the draft 2018 Surety Assessment is not similar in structure and format of the 2006 Surety Assessment. The previous assessment contained all analysis and recommendations within one section of the report with additional sections containing discussions on supporting and background information. This format allows for the easy identification of the results of the assessment and the factors used in the development of the analysis. Found below is a comparison of the table of contents of both assessments.

2006 Surety Assessment Report Outline

1. Introduction

2. NAESB Description

3. Objective and Purpose of NAESB Standards

4. Critical Success Factors

5. Metrics of Importance

6. Surety Assessment Research

7. Surety Assessment Analysis and Recommendations

7.1 Security Issues

7.2 Recommendations for NAESB Principles

7.3 Other Areas for Improvements

8. Summary

9. Conclusion

2018 Surety Assessment Report Outline

1. Overview

1.1 Background
1.2 Scope
1.3 Adversary Models and Attack Scenarios
1.3.1 Adversary Models
1.3.2 Specific Scenarios Considered

2. System Description and Analysis

2.1 ACA and Certificate Management
2.1.1 Description
2.1.2 Findings
2.2 Business Operations
2.2.1 Description

- Gas Sector
- Electric Sector
- EDI Cyber Attack

2.2.2 Findings
2.3 OASIS
2.3.1 Description
2.3.2 Findings

3. Conclusions and Recommendations for Future Assessment Activities

2.) The committee observed that the level of detail in the draft 2018 Surety Assessment is not consistent with the detail level of the 2006 Surety Assessment. As part of the previous assessment, Sandia National Laboratories provided a detailed analysis and recommendation for each finding. This format provided easily digestible action items NAESB used to determine how to address the assessment recommendations.

It appears as though the draft 2018 Surety Assessment still contains a disparate level of detail concerning the review of specific standards and the accompanying analysis. Provided below is an example of a finding, analysis and recommendation contained in the 2006 Surety Assessment and a similar finding, analysis, and recommendation contained in the draft 2018 Surety Assessment.

2006 Surety Assessment Report

7.1.1 Versioning of software and protocols

Recommended versions of software and protocols are addressed in several places in the standard. For example, Standard 4.3.61 states "Data communications

2018 Surety Assessment Report

2.2.3 Findings

Weakness – Low: NAESB standards contain references to specific versions of communication protocols that may be vulnerable to attacks discovered since the publication for Customer Activities Web sites should utilize 128 bit Secure Sockets Layer (SSL) encryption." There are also specific technical requirements for workstations listed in Appendix B.

Analysis: Specifically requiring versions of software or protocols creates the risk that these versions may become outdated or ineffectual before the standard is revised. It also leaves open the possibility that some necessary applications or protocols may not be addressed. If either of these occurs, vulnerable versions of software or protocols may be allowed by the standard. An attacker could take advantage of these vulnerabilities, or an insider could negotiate using a vulnerable version of an application and then exploit that vulnerability.

Recommendation: Where required versions must be specifically noted, it should be stated that the most current versions of applications and protocols are required, along with the latest patches. Sandia recommends that the NAESB standards not enumerate specifics for client workstations. Rather, it would be beneficial to refer to a well-known standards organization such as SANS6 or NIST7 and require that workstations conform to those standards for secure systems at some specific level. See the subsection 7.1.2 for additional information.

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 Appendix C: References to the SSL Protocol in Reviewed Documents.

Justification: Insecure protocols can allow an attacker to intercept or modify communications, or to impersonate the various parties involved in the communication. However, while insecure protocols are a high risk, the team downgraded it to "Low" for the following reasons:

1) Implementation details are outside the purview of NAESB. Since new security vulnerabilities are discovered every day, any organization implementing the NAESB standards will already have to consider any bulletins related to vulnerabilities in their hardware, software, configuration settings, and protocols. Even including references to the latest government or industry standards instead of specific versions will not address the "publication delay" between discovery of a vulnerability and an updated standard being issued.

2) The close relationship between organizations, the complexity of their internal systems, and humans in the loop, will allow malicious activity to be discovered relatively quickly.

Recommendation: To ensure outdated protocols do not provide a vector for future attacks, the assessment team recommends referencing the latest government or industry standards for secure communications instead of directly defining the minimum requirements. In addition, 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. For example, a standard could indicate that systems should use the latest IETF TLS standards within a certain number of days after they are published.

While NAESB made modifications to the WGQ/RMQ Quadrant Electronic Delivery Mechanism Related Standards in response to the recommendations made in the 2006 Surety Assessment, it does not appear that any modifications were made to this specific standard – Standard 4.3.61 – since the assessment. A similar recommendation is made in the 2018 report; however, in a much more generalized manner. It may be that Sandia National Laboratories did review this specific standard and did not identify it as presenting a vulnerability, given the changes in the cybersecurity space over the last decade. While Sandia National Laboratories did provide a table in Appendix C of the draft 2018 Surety Assessment that identifies the areas of the standards that reference SSL, there is no accompanying analysis to indicate that this standard or other specific standards were reviewed on an individual basis.

There are four additional areas of analysis identified in the 2006 Surety Assessment that appear to have not resulted in any additional modifications to the standards. The draft 2018 Surety Assessment does not contain discussion on these items, and in one instance, the draft 2018 Surety Assessment seems to contradict the 2006 Surety Assessment. The past assessment asserted a potential risk for abuse and identified a security vulnerability with the "refnum" data field. While the 2018 Surety Assessment does identify the "refnum" data field as a legacy functionality that may provide a vector for future attacks, the analysis specifically states that this is not a vulnerability in the standards and does not provide reasoning as to why the data field should no longer be considered as such.

2006 Surety Assessment Report

7.1.14 Refnum and Refnum-orig

The standard does not check on a Sender's abuse of Refnum & Refnum-orig.

Analysis: An adversary, on a "first send", could set Refnum-orig not equal to the current Refnum. The Receiver would then conclude that the Sender this was a resend—either first or second—and that the first send had been lost. Over time the adversary could claim unfair business practice on the part of the Receiver: the Receiver consistently drops the adversary's first send, making the adversary resend and thus lose valuable time, giving other trading partners an unfair advantage. Alternatively, the adversary could reuse Refnums.1 For example, the adversary could send payload A, proposing a deal favorable to the adversary, followed, sometime later, with payload B, proposing a deal favorable to the Receiver—both payloads sent with the same Refnum. When the Receiver accepts payload B, the adversary proceeds, fraudulently acting as though the Receiver had accepted payload A. When the Receiver protests, the adversary claims that the Receiver changed the Refnum in payload B in an attempt to cheat the adversary. There may be other ways the adversary can use Refnum to their advantage. The point is that the Standard requires that the "refnum data element is always unique over time" (IET page 175) but there is no provision for confirming compliance by an implementation. Compliance capability would require some algorithmic way to detect reuse, or a capability to cross reference Refnum fields with prior transactions.

Recommendation: A mechanism should be in place to prevent or detect the abuse and reuse of Refnum and Refnum-orig values

2018 Surety Assessment Report

2.2.3 Findings

Weakness – Low: NAESB standards contain legacy or deprecated functionality.

Justification: 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.

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.

The other three areas identified in the 2006 Surety Assessment that appear to have not been previously addressed and were not discussed in the draft 2018 Surety Assessment are as follows:

A. 7.1.17 Central Address Repository (CAR)[1]

Standard 4.3.19 states that the CAR should make available a consolidated repository of the Transportation Service Providers' current URLs listed in Standard 4.3.18 in two ways: (1) a vehicle to link to sites and categories, and (2) a downloadable list. The CAR is available to any Internet user. Standard 4.3.20 states that a userID or password should not be required to access the Central Address Repository or the Transportation Service Provider's Informational Postings web site.

Analysis: The CAR can be used as a target list for a malicious individual. Leaving the CAR unprotected and available to any Internet user can result in attacks being directed at the customers of a specific site. It is tailor-made for attacking using a denial-of-service type of attack. There was a similar item in the previous assessment. Due to increased threats on the Internet, the recommendation reiterated here.

Recommendation: Protect the CAR using SSL and basic authentication. It is recommended that the standard be reworded to state that a userID and password be required to access the CAR for security purposes. The access password can be a single userID/password combination created, and changed yearly, by NAESB for the member organizations, but implemented locally by each member. The userID/password can be distributed securely by the NAESB office to members.

B. 7.1.20 Message Replay Attacks[1]

Message replay is not addressed fully in the standards.

Analysis: Currently there is not a complete mechanism in place that will disallow replay attacks. Both client and server mechanisms need to be in place to keep this from being a viable attack. Timestamps could be spoofed, if not digitally signed, altering the outcome of a transaction. There are timestamps in the EDI/EDM transfer of files, in the header for example, but it's unclear if that is digitally signed, but we believe it is. That doesn't seem the case for all methods however, such as Batch FF/EDM. There was a similar item in the previous assessment. The tools are available for mitigation of this vulnerability and are readily available for use.

Recommendation: Ensure that all transaction methods include the timestamp in an area of the transaction that is digitally signed. If the resolution of the timestamp is not fine enough to ensure that only one transaction will be sent with that timestamp, an additional field containing a sequence number will be required such that the combination of the timestamp and sequence number field will always be guaranteed to be unique. This method will only work if the transaction is digitally signed using an accepted cryptographic checksum. An example of such a cryptographic checksum algorithm is the Secure Hash Algorithm defined in FIPS Pub 180-1. PGP uses several accepted cryptographic checksum algorithms, such as IDEA, RSA, DSA, MD5, SHA, and SHA-1. However, there have been demonstrated compromises for all but SHA-1 and as computing power increases, these compromises will become feasible for an attacker to perform within a few years.

C. 7.3.5 Definitive References[1]

The references should be definitive. For example, if the Standard recommends Dwight & Erwin's book on CGI, then the reference should not read "A source on CGI is…" as it does now, using an indefinite article, but rather should use the definite article, as in "The source on CGI is…" or "The recommended source on CGI is…"

[1] This information is found in the 2006 Surety Assessment.

3.) There are several statements made in the report that appear to be part of the surety assessment analysis but do not follow the finding – justification – recommendation format. As mentioned above, following this format will allow NAESB to easily determine the recommendations of Sandia National Laboratories and provide a starting point for discussions on determining the next steps. The table below captures the specific statements identified by the Chair and Vice Chair of the committee that contain inadequate analyses or recommendations.

2018 Surety Assessment
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. **Justification:** 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. (i.e. – It would actually have to be registered as a business in a valid state or country.) However, this would mean it is an actual organization, even if it is only set up as a front company. Once the organization passed these checks, the attacker would be able to gain read-only access to OASIS. **Recommendation:**
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. **Justification:** 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. **Recommendation:**
Finding: Nomination of, but failure to use, large quantity of capacity (and variations): **Justification:** 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, any excess capacity can be easily sold on the spot market. **Recommendation:**
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. **Justification:** From the on-site discussion, it was determined that there are a number of 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 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. The complexity of a cyber attack for this scenario, and an evaluation of the difficulty related to this scenario, can be found in Appendix D: Sample Attack Graph.

Recommendation:

Finding: An attacker able to steal an organization's certificate/credentials for OASIS: In this scenario, an attacker is able to obtain access to OASIS by impersonating an organization with legitimate access.

Justification: 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, and utilizing alternate channels to conduct business.)

Recommendation:

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.

Justification: 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.

Recommendation:

Finding: Backend system security: It was noted that the industry has purposefully chosen to not address this through the NAESB standards.

Justification:

Recommendation:

Finding: Overall, the assessment team did not identify any issues that were introduced by these proposed changes [to the ACA Accreditation Requirements].

Justification:

Recommendation:

Finding: Overall, while the gas and electric markets are complicated, and have many interdependencies, the nature of this complexity – as it relates to NAESB standards and business practices – increases the difficulty of successfully conducting a cyber attack in this area.

Justification: In many attack scenarios, even if an adversary could compromise an organization's private key, multiple systems at multiple organizations would also have to be compromised to hide malicious activity. In addition, multiple business and operations functions include a human in the loop, allowing detection of malicious activity. In the event minor activity did go unnoticed, it was indicated at the on-site meeting that most companies have a dispute resolution or customer dispute process that would allow remediation of any issues in a timely manner.

Recommendation:

Finding: For the first and second items of the tasking [review of NAESB Standards and Business Practices and review of NAESB PKI Program], the assessment team found that the NAESB Standards and Business Practices, and the PKI program, utilize industry best practices and are well-designed to prevent attacks against the gas and electric markets.

Justification:

Recommendation:

Finding: For the third task, the dependency between the gas and electric markets, from discussions with industry partners during the on-site meeting, it was determined that compromise of business operations in the gas sector, in the extreme, could cause minor, short-term commercial damage to gas operations, but that gas flow would not be interrupted, ensuring electrical generation would not be impacted.

Justification:

Recommendation:

Finding:

Justification:

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.

Finding:

Justification:

Recommendation: Perform security assessments on software that is used by large number of organizations to identify vulnerabilities that could be exploited by an attacker.

Additionally, there are statements in the draft 2018 Surety Assessment that appear to be a finding and a recommendation with a supported analysis but are not presented as such in the report. These are identified below and inserted into the finding – justification – recommendation format.

Finding: A third-party platform provided the attack vector in the EDI cyber attack. Reliance on third-party software and hardware – such as those from Microsoft, Cisco, or a Linux distribution – is necessary in today's business environment.

Justification: However, critical vulnerabilities are often found in these products, affecting any organization using these products in their operations. In addition, even utilizing security software can result in additional attack vectors as was the case with the FireEye security appliance.

Recommendation: However, applying industry best practices throughout an organization can help mitigate the effects of these vulnerabilities. In this case, separation of the business and operations networks – and the ability to use backup procedures – allowed the organizations affected to continue operations despite the loss of their EDI platform.

Finding: Given the type and amount of information that is posted on OASIS, it is possible that a malicious actor could establish themselves as a legitimate business, register in the Electric Industry Register (EIR), and then request an OASIS account – which would allow them to view this sensitive information.

Justification: However, the NAESB OASIS Subcommittee engages in constant discussions with their members and FERC to ensure there is a balance between protecting this information and meeting industry needs.

Recommendation: While this could result in an adversary gaining access to sensitive information, since it is driven by federal regulations, and constantly considered by the NAESB OASIS Subcommittee, the team "downgraded" the weakness to an observation.

Finding: NAESB standards enumerate the requirements of OASIS nodes, but does 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. (A deliberate decision was made to not address this through NAESB standards.)

Justification: 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.

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

4.) The committee asked for specific information on any potential gaps or vulnerabilities and recommendations for mitigation. While the information provided in Appendix D: Sample Attack Graph is helpful, additional details are needed. The report notes that "an attack directed against a business network – such as the Shamoon attack used against Saudi Armaco in 2012 – would be more likely" but does not provide background information on why this type of attack may be more likely or how to mitigate. Without this type of assessment, it will be difficult to determine the adequacy of the current standards to protect against such an attack.

5.) Finally, the committee requested that Sandia National Laboratories describe the scenarios considered as part of the surety assessment and any potential economic or reliability consequences. The revised draft does identify the five scenarios considered by the team in the development of the surety assessment but fails to address any reliability considerations. The feedback provided by the committee specifically highlighted how a commercial attack could impact reliability. It would be beneficial if the report could include discussion on potential reliability impacts as noted by the committee.