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

15 Jul 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

This page intentionally left blank.

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 covers the threat-based analysis performed by the Sandia National Laboratories' (SNL) Information Design Assurance Red Team (IDART™), discusses several real-world attacks affecting the gas and electric markets, and discusses additional areas that were of concern to members of the NAESB Critical Infrastructure Committee.

This assessment was executed by IDART 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 an assessment regarding the cybersecurity posture of specific areas of the wholesale and retail aspects of the gas and electric markets; provide awareness of various attacks that have occurred; and to provide information and cybersecurity resources related to future operations – specifically the increased threat surface from an increase in automation, and the integration of new technologies into operations.

Results from the overall assessment are included in the other reports that were delivered under this program, with this report serving an informational purpose as opposed to an assessment purpose. If information regarding the surety assessment findings are desired, the assessment team recommends interested parties review those other reports.

1 Overview

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 covers the threat-based analysis performed by the Sandia National Laboratories' (SNL) Information Design Assurance Red Team (IDART™), discusses several real-world attacks affecting the gas and electric markets, and discusses additional areas that were of concern to members of the NAESB Critical Infrastructure Committee.

1.1 Assessment Scope

Given the expanse of NAESB's standards, and their reach into many different areas of the various markets, this assessment was limited to three specific tasks:

1. Review of NAESB Standards and Business Practices
2. Review of NAESB PKI Program
3. Dependency Analysis Between the Gas and Electric Markets

These three tasks involved a review of the following documents:

- Internet Electronic Transport Related Standards, Version 3.0
- RXQ.7 – Internet Electronic Transport Model Business Practices, Version 3.1
- WGQ Quadrant Electronic Delivery Mechanism Related Standards, Version 3.0
- RXQ.5 – Quadrant-Specific Electronic Delivery Mechanism Model Business Practices, Version 3.1
- WEQ-012 Public Key Infrastructure, Version 003.1
- Accreditation Requirements for Authorized Certification Authorities – February 18, 2014
- NAESB Authorized Certification Authority Process – December 8, 2016
- Updates to the Accreditation Requirements for Authorized Certification Authorities document that were provided on September 07, 2017

In addition, the following documents were added to the assessment based on information gathered during the assessment activities:

- GlobalSign Certification Practice Statement v8.6, December 15, 2017
- OATI webCARES Certification Practice Statement v3.3, October 2017
- 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

The results of the surety assessment regarding these business practices, standards, and other documents, can be found in the surety reports that were delivered as part of this assessment activity.

During the assessment timeframe, real-world events included the EDI cyber attack that occurred in April 2018. As a result, NAESB requested the assessment team review publicly available information and provide feedback regarding the attack. This feedback is included in Section 2.3.1.

In addition, during various discussions with the NAESB Critical Infrastructure Committee (CIC), members of the CIC identified other areas where more information would be of interest. While these areas are beyond the scope of this assessment, the program manager, Mr. Christopher Freitas, indicated that he is open to funding requests from NAESB if there are emerging technologies or other areas that need to be investigated. However, to provide some information related to these areas, the assessment team has provided a list of resources that can be used by organizations looking to adopt these new technologies. These references can be found in Section 3.1 .

2 Current Operations

This section provides a description of current operations, a threat assessment against those current operations – including a brief discussion on threat models.

2.1 Description of Current Operations

This section provides a description of current operations – divided into the areas of Authorized Certificate Authorities and Certificate Management, Business Operations, and the Open Access Same-Time Information System (OASIS). This description is provided as it provides the basis for the threat assessment found in Section 2.2.

2.1.1 Authorized Certificate Authority (ACA) and Certificate Management

This subsection covers the description of how an ACA is established, how an organization obtains a NAESB Certificate from an ACA, and how these certificates are revoked and/or reissued, if necessary.

Description

GlobalSign and OATI, which are the NAESB Authorized Certificate Authorities (ACAs).[1,2] GlobalSign is a multinational company that is headquartered in Belgium; however, they do have a U.S. Regional Office based in Portsmouth, New Hampshire. OATI is headquartered in Minneapolis, Minnesota.

To be designated as an ACA, an organization must meet the requirements found in the *NAESB Accreditation Requirements for Authorized Certification Authorities.* This document includes requirements for vetting individuals or organizations, issuance of certificate revocation lists, roles of key personnel, system monitoring and auditing, and other critical functions. If an organization meets the accreditation requirements defined by NAESB, they can then follow the certification process as described in *NAESB Authorized Certification Authority Process.* The certification process requires the organization submit the appropriate paperwork to NAESB to prove they meet the requirements. This paperwork includes the results from audits performed by appropriate, third-party organizations to ensure compliance with NAESB requirements. In addition, to be an ACA, the organization must be registered in the EIR.

To illustrate how an individual or organization would obtain a valid certificate, here are the steps for obtaining a certificate from GlobalSign:

1) Entity Establishes a GlobalSign Account: This includes submitting the entity's information, identifying the administrator for the account, and establishing a username and password for GlobalSign's system.
2) Provided Information is Vetted by GlobalSign: Vetting of information is done in two parts. The first, organizational level verification, is performed in accordance with Section 3.2.2 of the GlobalSign CPS: *Authentication of Organization Identity*. The second, individual identity

[1] Systrends is another NAESB ACA but processes its certificates through GMO GlobalSign Inc. and was not independently reviewed.

[2] SSL Corp. d/b/a SSL.com was certified as an ACA in July 2018, which was outside the time frame considered in this report.

verification, is performed in accordance with Section 3.2.3 of the CPS: *Authentication of Individual Identity.* Section 3.2.3 includes NAESB specific information in Subsection 3.2.3.5: *North American Energy Standards Board (NAESB) Certificates*.

3) Certificate Issuance: Once the provided information has been vetted, the key generation is performed in the applicant's browser, the certificate is generated in a secure manner, and delivered to the applicant via the previously provided email address (or other equivalent method.)

Similar processes for certificate issuance, including NAESB specific requirements, can be found in the OATI CPS.

Revocation of certificates is covered in both the GlobalSign CPS (Section 4.9) and OATI CPS (Sections 3.4.5-10). Both documents include the conditions for revocation, and who can request revocation. GlobalSign will process a revocation within 24 hours of a revocation request; OATI will begin an investigation on a request for revocation within 24 hours; and will place revoked certificates within the CRL within ten minutes of the certificate being revoked.

Other information included in the OATI and GlobalSign CPS's include: Physical protections, cryptographic security, protection of key materials, personnel vetting, logging, log retention, and other processing requirements. In general, these requirements are designed to protect critical cryptographic information and systems against advanced adversaries.

In the event of a compromise of an ACA's private key, subscribers have the option of obtaining a certificate from the other ACA. Alternatively, the subscriber can wait to obtain a new certificate once the ACA has recovered from the compromise. The ACA recovery process, which includes generating new keying materials, takes approximately one week.

2.1.2 Business Operations

This subsection will provide a description of the way operations are conducted in the gas and electric sectors, as they relate to the NAESB standards being reviewed, and as understood by the assessment team.

Description

The standards and business practices that are developed by NAESB are voluntary, and NAESB does not have any regulatory role in the gas or electric sectors. However, in the wholesale markets, WEQ and WGQ standards are filed with the Federal Energy Regulatory Commission (FERC). Almost all the WEQ and WGQ NAESB standards have been adopted by FERC and have been incorporated by reference into mandatory federal regulations. In addition, for the retail markets, the RMQ standards are made available to state utility commissions through the National Association of Regulatory Utility Commissioners (NARUC). A number of these standards have been adopted by state utility commissions or have served as the basis for their own regulations.

Gas Sector

For wholesale gas transactions, there are two methods for shippers and pipelines to interact: the pipeline's electronic bulletin board (EBB), and electronic data interchange (EDI). For EDI, the communication is secured using file-level encryption via PGP. To access an EBB, a user must have a valid username and password, and the communication is secured with SSL (or TLS) since commercially sensitive information may be exchanged.

In addition to gaining access, an organization that wishes to conduct business with a pipeline must establish their creditworthiness before being allowed to participate in the nomination process. This vetting process takes 10-30 days, and serves two purposes:

1) To validate the new organization is a legitimate business
2) To establish capacity limits so shippers do not overschedule capacity

Once this vetting has been completed, a shipper is able to use the pipeline's interfaces to participate in nominations and capacity scheduling.

There are five nomination cycles in each calendar day: Timely Nomination, Evening Nomination, and three Intra-Day Nominations. The Timely and Evening Nominations are effective for the next calendar day. These nomination cycles establish the times when organizations can submit nominations, when nominations are confirmed, schedules are issued, and gas flow will begin.

The confirmation process ensures that upstream and downstream flows are coordinated to ensure alignment. (i.e. – A pipeline won't allow 10,000 units to flow into it unless there is a confirmed downstream destination for those 10,000 units.) In addition, the nominations are reviewed to ensure that gas is being delivered to a location that is identified in a contract, as gas cannot be diverted to a new location. Finally, once these requirements have been confirmed, an additional process allocates the available capacity based on service level agreements and other aspects of established contracts. Once the verification and prioritization are completed, the new schedule is released. The Gas Sector scheduling process is illustrated in Figure 1 below.

Figure 1 - Gas Sector Scheduling

It is important to note that, collectively, these steps act as a series of security checks and together add layers to a defense-in-depth posture. The various steps of the nomination process use multiple systems and software, and each account is tied to a specific contract which is handled by a specific person. The result is a personal level of involvement in the various business relationships between shippers and pipelines. This personal level of involvement means that large changes (increases or decreases) in nominated capacity would be noticed almost immediately as it would be outside the normal or expected

behavior for that specific customer. The length of the nomination cycle phases would allow these issues to be identified and remediated within the same cycle.

The pipeline system itself is fairly robust and, in the event an attacker managed to arrange for an oversupply of gas to be diverted into a pipeline, it would not result in a catastrophic failure. As discussed in the on-site meeting, while the commercial impact could last approximately 3 days, gas would continue to flow during that period, mitigating widespread impacts. On the opposite end of the spectrum, where there is an undersupply of gas, this is noticed fairly quickly and unused capacity can be resold on the spot market. This market has a strong demand since there is a large difference between the cost of firm gas service and interruptible gas service. During the on-site meeting this cost difference was described as "pennies on the dollar". Finally, in the event of drastic undersupply, pipeline companies have procedures to divert gas into a pipeline to avoid vacuum until normal operations are resumed.

If an organization discovers a key compromise, it is handled at the trading partner level. The impact of this compromise will depend on the policies of the organization that had its key compromised, and whether it has a unique key for each trading partner or reuses the keys for multiple partners. However, if the trading partners use the NAESB Trading Partner Worksheet (TPW), they will have the contact information – including after-hours contact information – for both trading partners. This would allow the organization to notify their trading partner of the compromise, and includes other information, such as a fax number, that could be used until a new key can be generated and shared with the trading partner. Finally, if the compromised key was used to make malicious nominations, electronic flow monitoring (EFM) exists at all interconnects, allowing organizations to determine where the gas was transported and allowing the use of a remediation process to address any issues.

Electric Sector

The Open Access Same-Time Information Systems (OASIS) is used to secure the right-of-way on a transmission line. This is a large system in terms of users, transactions, and transaction value. OASIS is used by over 150 transmission providers to sell capacity to over 1,100 additional entities. However, entities can be more than a single user, and there are 8 entities that have over 100 OASIS users. In one month, one of the larger providers logged over 160,000 transactions worth approximately $5 million and, industry wide, transmission costs are approximately 10% of the transactional costs for the purchase of energy.

To access OASIS, an organization 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

Once it is verified that the organization is in the EIR, and has a valid certificate from an ACA, a one-time password for the OASIS system is emailed to the contact information provided in the request. Logging in

with the one-time password automatically brings the user to a “reset password” page. Initial access to OASIS is on a read-only basis, and a user or organization must establish agreements with other organizations who then authorize the new organization to start trading with them.

If user or organization credentials and certificates were compromised, and malicious activity conducted, it would be up to the compromised party to identify and remediate the situation. Transmission providers are not involved in merchant activity and will generally allow any activity that has been previously authorized, removing them from any mitigation role. However, to support remediation, most companies have a customer dispute/dispute resolution process.

2.1.3 Open Access Same-Time Information Systems (OASIS)

Description

OASIS was established by the Federal Energy Regulatory Commission (FERC) in 1996 to ensure that all entities wishing to obtain electric power transmission services could have equal access to necessary information and services. To support this, OASIS serves two purposes: 1) To provide a location where an entity can request services from a transmission operator, and 2) Provide the information necessary for an entity to conduct business in the wholesale electric quadrant.

To support (2) above, FERC requires certain information to be posted to OASIS to allow users to make requests for services, enable business decision making, etc. This information can include sensitive infrastructure information such as transmission models, system planning or facilities studies, transfer capacity, and interconnections. In addition, transmission providers must post their rules, standards, and practices relating to transmission services. Specific requirements for posted information can be found in the Code of Federal Regulations (18 CFR 37.6 *Information to be Posted on the OASIS*.)

The architecture of OASIS is not as a single system, but as a network of OASIS “nodes”, where each node provides the required services and information for transmission providers in the appropriate geographic region. Each node is required to meet FERC requirements and provide a secure, Internet-connected portal that entities can access with a web browser. While all nodes must be connected through the Internet, it is also allowed for nodes to have separate interconnections. Regional Transmission Organizations (RTO) and Independent System Operators (ISO) then use these nodes to provide the required services and information.

While nodes may be interconnected, per discussions during the on-site visit, federal regulations prevent OASIS from being connected to any control systems. However, this requirement is out of scope for this assessment, and attack vectors requiring interconnection between these systems were not considered.

Any appropriate party may obtain OASIS access as detailed in Section 2.1.2. To obtain access to a transmission provider’s information, in addition to meeting the transmission provider’s requirements, they must also provide appropriate information to the transmission service information provider (TSIP). This information is detailed in *NAESB Open Access Same-Time Information Systems Business Practice Standards and Communication Protocol (S&CP)*, Section 002-3.1.

NAESB has created standards for communication within OASIS, including templates for uploading and downloading of files; a complete data dictionary for data elements used in OASIS – including size constraints, data types, and allowable (or prohibited) values; and state diagrams for how to process various transactions and requests. However, if there are different requirements found within a transmission provider's FERC approved tariff, those will take precedence over the NAESB standards.

2.2 Threats Against Current Operations

This section discusses several adversary models that can be used to understand the capability of adversaries (and some models that also consider intent); attack scenarios against the business practices and standards that were reviewed by the assessment team; and an overview of several real-world attacks that may be of interest to NAESB organizations.

2.2.1 Adversary Models

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. For example, one high-level and generic adversary model is the Defense Science Board's Taxonomy of Cyber Security Adversaries, which defines three levels and six tiers of capability. These range from Tier I, where an adversary has to rely on published exploits; to Tier VI, which is a nation state adversary capable of using their cyber capabilities in conjunction with their military and intelligence capabilities.[3] A breakdown of these levels and tiers can be found in Figure 3 in Appendix A.

A second generic adversary model is the Sandia National Laboratories' Generic Threat Matrix, which defines eight levels of adversary, with each level of adversary having different capabilities in attributes such as: time dedicated to an attack, number of technical personnel, cyber knowledge, kinetic knowledge, and several other characteristics. The matrix with these attributes can be found in Figure 4 in Appendix A.

An electric-sector-specific adversary model is discussed in the Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector report by the Mission Support Center at Idaho National Laboratory.[4] This report discusses specific threat actors, including Russia, China, Organized Crime, and several others. For each of these specific threat actors the report includes a description of capabilities and a list of attacks attributed to that threat actor.

Finally, ICF International published their analysis in: Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats.[5] This breaks the adversaries into two categories: State and non-State Actors, and Insider Threats. This report also provides a brief description of both classes of threat.

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

[3] Defense Science Board, Task Force Report: "Resilient Military Systems and the Advanced Cyber Threat", January 2013, Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics.

[4] https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector.pdf

[5] https://www.energy.gov/sites/prod/files/2017/01/f34/Electric Grid Security and Resilience--Establishing a Baseline for Adversarial Threats.pdf

identified attack vectors to be exploited. In addition, a generic threat matrix eliminates any classification concerns when associating specific groups with their capabilities.

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.

2.2.2 Attack Scenarios Against Current Operations

The team used the provided NAESB standards and business practices, their knowledge of current cyber threats, trends in attacker behavior, and their subject matter expertise to identify potential attack paths related to the NAESB standards. Consequences of concern for internet electronic transport security requirements include four primary (PAIN) security aspects:

- Data Privacy: unauthorized parties cannot decipher the content of the data.
- Authentication: the Receiver is certain of the identity of the Sender.
- Data Integrity: unauthorized parties cannot modify or corrupt the data.
- Non-repudiation: the Sender cannot deny ownership of the transaction if it was sent with their digital signature.

From the list of potential attack paths identified by the team, the assessment team logically grouped them into the scenarios below. For example, if the team identified several ways to perform a denial of service attack 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.) these were grouped into the "malicious modification of nominations" scenario.

It should be noted that the IDART attack analysis is conducted by a multi-disciplinary team executing an orchestrated brainstorming session. Such a session will develop an attack graph that is a function of the identified adversaries, access points, multiple potential adversary exploits as executed against the targeted system and ultimately the attacker goals. A good description of an attack development and analysis process can be found in the SANS Institute - The Industrial Control System Cyber Kill Chain[6]. This process breaks down the attack into logical steps including planning, attack preparation, intrusion, command and control and, finally, attack execution. Yet another developed and widely-recognized framework is the MITRE ATT&CK™[7]. It is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The MITRE knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

[6] SANS Institute, "The Industrial Control System Cyber Kill Chain". Michael J. Assante and Robert M. Lee, October 2015.
[7] https://attack.mitre.org/

The scenarios described below including mitigating factors that would prevent an attack – or at least make an attack significantly harder. Figure 2 contains representative classes of attacks which could be used to accomplish the associated scenarios (given specific access and authorizations assumptions). In addition, Figure 2 also illustrates how the scenarios relate to each other, the NAESB-responsible processes involved in the scenarios, possible consequences, and support the defense-in-depth analysis that was conducted by the IDART team.

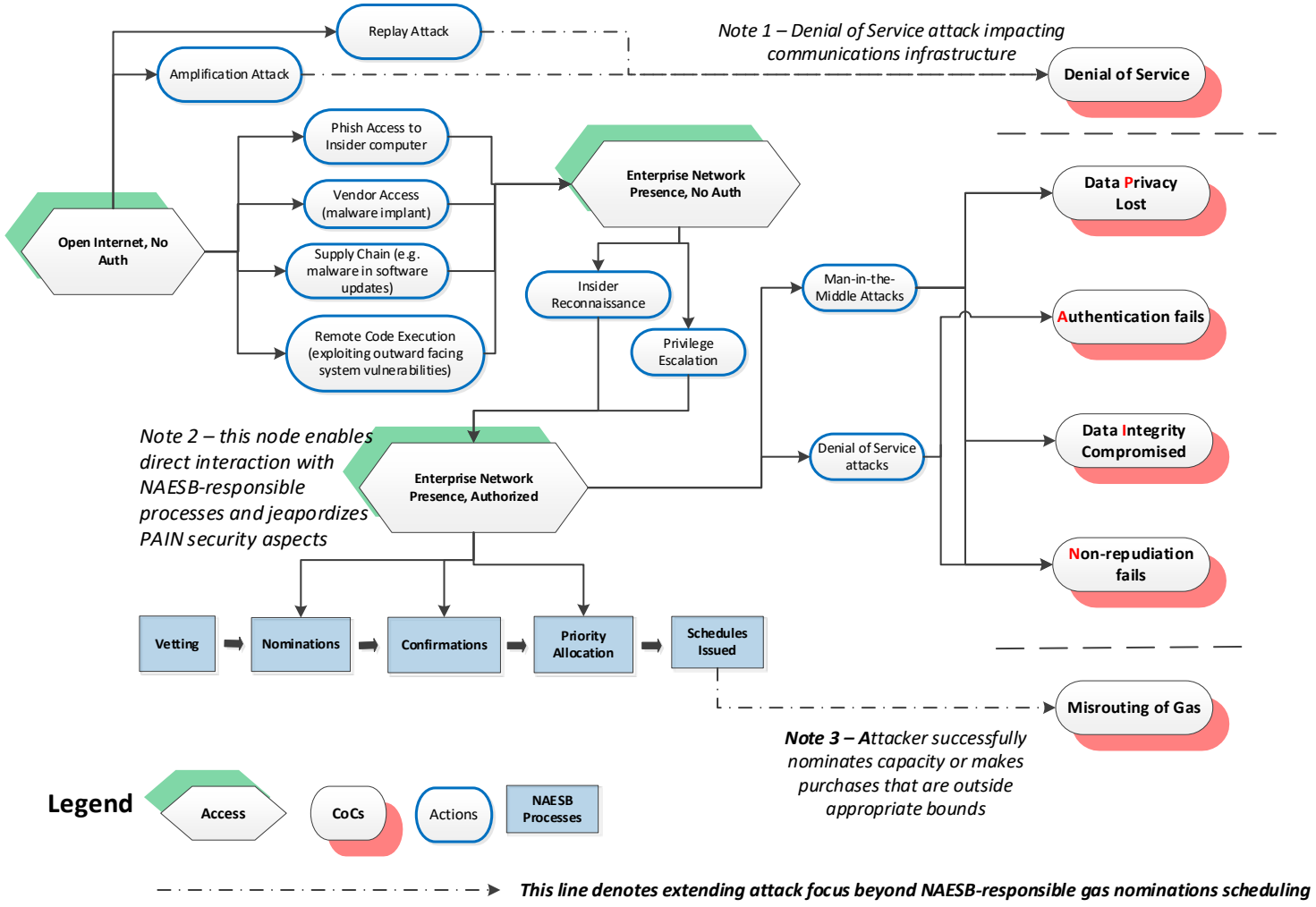

Figure 2 - Gas Sector Scenarios

1) Malicious modification of nominations: This scenario can involve the modification of a nomination or a denial of service (DOS) against the submission of a nomination. The DOS attack is described in the Business Operations Report[8] and impacts the relevant communications infrastructure rather than the NAESB-responsible processes, as shown in Figure 2 (Note1).

[8] Presented to the Critical Infrastructure Committee in June 2019 and now submitted for final review.

The modification of a nomination can be quite long depending upon the attacker access and authorization. For example, if the attacker starts from the *open internet without authorization*, he could use an email phishing attack (or other classes of attack) to gain unauthorized access to the business network. From this logical node, the attacker can begin to conduct reconnaissance, steal credentials, or attempt to escalate privileges to gain "authorized" access to processes that enable gas sector nominations. This same node (Enterprise Network Access with Authorization) is the *starting state* for a technical insider attacker with presence on the enterprise network and appropriate authorizations.

This node is an important enabler for reconnaissance of the gas nominations process as it directly enables an attacker to learn vital information. Directly from this access node, all (PAIN) security aspects for internet electronic transport security are directly achieved by an attacker (Note 2). In addition to disrupting individual gas nominations processes (e.g. nominations, confirmations, priority allocation), this node supporting further exploits as shown in Figure 2. Two classes of attacks were considered based on the review of the NAESB processes:

- Man-in-the-middle attack: Can be initiated and accomplished through email phishing attacks perhaps using hyperlinks requesting information from employees. This information capture can be leveraged to identify known Operating System or application vulnerabilities to control an access-enabled machine. From there, privilege escalation can be accomplished through social engineering to gain privileged access on the network. Once that is accomplished a threat actor can establish a presence to intercept, spoof, or corrupt data; or steal data for other malicious purposes, creating issues with Data Privacy, Data Integrity, and Non-repudiation which are all principles required for successful transaction security. For example, a loss of data integrity can create issues with process nominations, confirmations, or priority allocation resulting in schedule issues.
- Denial-of-service attack: Could potentially be accomplished through data flooding by corrupting data packets, creating a high-volume of error messages preventing valid nominations from being accepted; spoofing valid transaction identifiers; or blocking authentication or confirmations within the process. These types of attacks can affect things such as authentication and non-repudiation with false or corrupted data sets.

However, achieving this node does not guarantee a successful malicious modification of nominations. From the on-site discussion[9], 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. It was also noted that the relationships between organizations are generally assigned to specific individuals, resulting in the individual being aware of normal business needs and requirements. Finally, the distributed nature and

[9] "Meeting with Sandia National Laboratory", minutes from Caroline Trum, NAESB Deputy Director, 8 August 2017

configuration differences of the trading partners adds difficulty to a potential large-scale attack and helps to limit impact attack.

2) A pipeline could be stressed by over supply or over purchase of gas: This scenario could extend from the modification of nominations scenario above, or from an attacker that is able to impersonate the organization. The control systems involved in the attack are not NAESB-responsible as see Figure 2. The attacker successfully nominates capacity or makes purchases that are outside appropriate bounds. A detailed description of this attack is in Appendix B. In this scenario, the defense-in-depth analysis 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.
3) 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.
4) 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.
5) 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.)
6) 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.

7) 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.

To illustrate the complexity and difficulty of conducting a successful attack, a high-level attack graph is provided in Appendix B: Attack Graph. This attack graph is not specific to the business processes of any organization, rather it references the general business operations that need to occur in a transaction.

2.3 Real-world Attacks

This section describes two real-world attacks that have been conducted against critical infrastructure systems, including an example for an attack against an IT-oriented network (EDI Cyber Attack) and one against an OT-oriented network (Ukrainian Power Grid Attack).

2.3.1 EDI Cyber Attack

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. [10,11]

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. 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.

During this attack, it was widely reported that, while the data systems were affected, operations were not impacted due to continuity of operations plans (COOP) that were utilized during the outage. Based on the information available, it is unknown whether EDI message processing functionality was the attack vector; or if other features and services provided by the platform were used to conduct the cyber attack.

In this case, COOP procedures were sufficient for organizations to maintain operations, despite losing their EDI platform. The assessment team has not been provided any information related to increased costs due to this outage; however, in general, information systems are used to provide more efficient and lower cost methods of conducting business transactions. Since these systems were forced offline due to the cyber attack, it is assumed that affected organizations, and those doing business with them through the EDI system, did face increased costs to conduct business.

[10] Threat Post. Insecure SCADA System blamed in Rash of Pipeline Data Network Attacks. https://threatpost.com/insecure-scada-systems-blamed-in-rash-of-pipeline-data-network-attacks/130952/

[11] Bloomberg. Energy Transfer Says 'Cyber Attack' Shut Pipeline Data System. https://www.bloomberg.com/news/articles/2018-04-02/energy-transfer-says-cyber-attack-shut-pipeline-data-system

In addition, stock prices for some of the affected organizations were down the day following the attack, which some reports attribute to the news of the cyber attack.[12] Assessing how much, if any, of this price fluctuation is due to reports of the cyber attack is outside the assessment team's area of expertise.

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.

The assessment team conducted a review of the reporting requirements from the Electricity Information Sharing and Analysis Center, the NERC CIP-008-5 Cyber Security – Incident Reporting and Response Planning Reliability Standards, and the Transportation Security Administration's Pipeline Security and Incident Recovery Protocol Plan. The review also extended to consideration of commonly used industry or commercial best practices and existing federal organizations that are available to respond to a cyber attack – including those that identify specific roles and responsibilities. This analysis determined that:

1. Both NERC and TSA require organizations to develop cyber security plans which include incident response,

2. NAESB has a strong need to get cyber incident information to both respond to threats and protect assets, and

3. Existing federal support for a cyber attack is strong and multi-faceted.

[12] Ibid.

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

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

> Note - There are a large body of examples to draft from because large commercial entities already have incident reports that address the needs of their industry. For instance, the financial industry will have a security incident report that favors quantification of exfiltrated personal/business data, portfolio strategies and factors that affect the entities ability to perform transactions; whereas a law firm would choose client confidentiality as high priority items to include in an incident report. These templates can be customized with relevant predefined items of concern. These reports can take the shape of a wizard driven reporting mechanism that populates a database such as the US CERT[13], DHS[14] and DOE[15] incident report portals or develop your own document using guidance from NIST Computer Security Incident Handling Guide.

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

2.3.2 Ukrainian Power Grid Attack

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.[16]

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

[13] US-CERT Incident Reporting System, https://www.us-cert.gov/forms/report
[14] Report Cyber Incidents, https://www.dhs.gov/how-do-i/report-cyber-incidents
[15] DOE - JC3 Incident Reporting, https://tickets.ijc3.doe.gov
[16] https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyberattack

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.[17]

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 connection 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) regarding the incident, and this report provides a brief description of the event, and recommended mitigations. [18] 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". Also of note is that they recommended contingency plans for continuity of operations and system shutdown. The full list of recommended mitigations, as well as links to other resources, can be found in the ICS-CERT report. In addition, ICS-CERT maintains a "Recommended Practices" site that provides additional guidance on securing OT networks, including any connections to IT networks.[19]

Recommendations: Specific to NAESB standards, the WEQ-002-5.1.1 authentication method is considered adequate and consistent with current business practices. WGQ Standard 4.3.60 and WGQ Standard 10.3.16/RMQ Standard 7.3.16 both allow basic authentication; however, the assessment team recommends multi-factor (e.g. two-factor) authentication be required on *an individual basis*. Simply authenticating the nodes involved is not acceptable.

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

[17] https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
[18] https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01
[19] https://ics-cert.us-cert.gov/Recommended-Practices

- Some related information must be made publicly available and this must not be blocked by the whitelisting implementation.
- Since NAESB standards do not specify the environment there could be negative impacts to non-EDI applications which are hosted on the same servers.
- The whitelisting decision must consider the support environment. The point being that if a legitimate transaction is blocked by the whitelisting, how quickly could the error be corrected given coverage and capability of the support team?

3 Future Trends and Areas for Analysis

This section discusses future trends in operations, and some of the technical areas that are expected to be adopted in the future. While these areas are outside the scope of the current assessment, the program manager, Mr. Christopher Freitas, encourages NAESB to engage with him to identify areas that should be investigated in future assessments. This section includes references to government resources that can be used to ensure secure implementations of these new technologies but does not contain the results of any assessment activities. In addition, this section includes possible NAESB actions for future investigation.

3.1 Trends in Operations

One of the key trends in listed in Deloitte's "2019 Power and Utilities Industry Outlook" is the use of technology to improve operations.[20] 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, real-time communications, and the increased connectivity between business and control operations (IT and OT networks) are adopted, these create new cyber security challenges and could provide an adversary with an attack vector against utility companies. *Irrespective of cyber attacks, new technology implementation should be evaluated for the introduction of new fault mechanisms; and new contingency plans should be developed in considerations of these potential new faults.* An important example would be the consideration of moving NAESB-responsible functions to a central cloud-based provider. On the surface this has many obvious benefits including standardizing the technology implementation, but it also introduces other potential risks. The importance of this was highlighted by a recent outage of the Google Cloud[21]. In the example of the EDI cyber attack (section 2.3.1), business operations could still be conducted despite the attack. Such a move might also open the door to cyber attacks and the leaking of organization information in the form of Shadow IT and Shadow Data[22].

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

[20] https://www2.deloitte.com/us/en/pages/energy-and-resources/articles/power-and-utilities-industry-outlook.html

[21] https://www.cbsnews.com/news/google-cloud-outage-hits-youtube-gmail-snapchat-apps-services-today-2019-06-02-live-updates/

[22] https://diamondit.pro/cybercrimes/shadow-it-and-shadow-data-how-organizations-can-protect-against-the-use-of-unsanctioned-applications/

have a method to disconnect the equipment from the control network and conduct manual operations until normal operations can be restored.

3.2 Government and Industry Standards

To address the security of the various emerging technologies such as those listed above, the assessment team recommends that organizations utilize the government and industry standards that are relevant to the technologies deployed. For example, NIST provides a number of whitepapers and standards related to cloud computing. These standards can be found at the NIST Cloud Computing Related Publications page and include special publications from the 500 and 800 series, and a variety of NIST cloud computing research papers.[23] Some of the documents referenced on this page are:

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

NIST also maintains a page related to the Internet of Things (IoT) that includes reports related to trust, fog computing (cloud computing for IoT), and other areas related to the IoT.[24]

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

- NIST 800-124rev1: Guidelines for Managing the Security of Mobile Devices in the Enterprise[25]
- NISTIR 8144 (DRAFT): Assessing Threats to Mobile Devices and Infrastructure - The Mobile Threat Catalog[26]
- NCCoE Project: Mobile Device Security: Cloud and Hybrid Builds[27]

3.3 Emerging Technologies

The NAESB CIC has tasked the assessment team to identify actions or areas of standards development that NAESB should be evaluating to ensure that the standards continue to address secure communications across new platforms.

This topic has been an area of ongoing dialog with our NAESB stakeholders, including the sharing of a list of technologies that are currently under consideration by the new Board Digital Committee as part of their efforts. This dialog has yielded the following list which were chosen as the most potentially informative to the CIC. The list is separated into those topics under energetic and differentiating development at Sandia (# 1 to 6) and topics important for NAESB but not necessarily an area of lab capability (7 and 8):

1. Distributed ledger technology (DLT) is an area of active work for both NAESB and SNL. In fact, the Sandia team has already delivered a whitepaper which discusses DLT (overview

[23] https://www.nist.gov/itl/nist-cloud-computing-related-publications
[24] https://www.nist.gov/topics/internet-things-iot
[25] https://csrc.nist.gov/publications/detail/sp/800-124/rev-1/final
[26] https://www.nccoe.nist.gov/sites/default/files/library/mtc-nistir-8144-draft.pdf
[27] https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/cloud-hybrid

and benefits) and important recommendations for the potential NAESB effort to convert the NAESB Base Contract into a smart contract. The white paper also described Sandia internally-funded research which is investigating using design/prototype multi-party computation (MPC) in a smart contract setting. The whitepaper also included potential Sandia support roles.

2. Distributed Energy Resources – focused on communication protocols. Sandia facilities include the Distributed Energy Test Lab[28] (DETL) which conducts research with industry and academic partners to integrate emerging energy technologies into new and existing electricity infrastructures. DETL research specifically includes cyber security of emerging distributed energy resources and related on communication protocols.
3. Data Analytics – this is an area of massive lab capability and investment. With respect to traditional internet communications analysis and detection the lab helps develop and implement novel defenses for both government and military networks. This effort includes advanced analysis for emerging threats and attack techniques. Sandia leads the national laboratory modeling and simulation in the development of a suite of network emulation and analysis capabilities collectively referred to as Emulytics™ (a holistic approach to system emulation and analytics)[29]. Over the last decade, we have developed and deployed a suite of cyber emulation, modeling, and analysis tools that support uses including predictive simulation, training, test & evaluation, and resilient system design.

   Emulytics™ experiments provide safe and isolated environments to study and test computing and communications systems and to exercise and train cyber staff. Enterprise computing and control systems environments are well supported today and we are developing support for emerging mobile computing and Internet of Things environments. Emulytics environments scale well and can be deployed on systems as small as a laptop and on clusters with hundreds of high performance servers. Our methodologies support the application of the scientific method to the study of cyber systems, and our tools make it easier to design, deploy, and collect data from virtualized experiments rapidly, reliably, and repeatedly.
4. Machine Learning – a method of data analysis that automates analytical model building. It is a branch of artificial intelligence based on the idea that systems can learn from data, identify patterns and make decisions with minimal human intervention. Machine learning was the focus of a recently completed grand challenge laboratory directed research and development effort[30].
5. Behavior Analytics – a tool that reveals the actions users take within a digital product. It organizes raw event data such as clicks into a timeline of each user's behavior, also known as a user journey. At Sandia, researchers model both malware and attacker behaviors to identify malicious activity. For example, Sandia scientists used virtual machine (VM)

[28] https://energy.sandia.gov/about/facilities/
[29] https://www.sandia.gov/emulytics/
[30] https://www.sandia.gov/news/publications/lab_accomplishments/articles/2018/adv_science_and_tech.html

technology and a supercomputing cluster to watch how botnets work and explore ways to stop them.[31]

6. Software Defined Networking (SDN) – approach to network management that enables dynamic, programmatically efficient network configuration in order to improve network performance and monitoring making it more like cloud computing than traditional network management. SDN was recently adapted into a Sandia patented alternative reality which can be deployed as a network defense. The capability is knows as HADES (High-fidelity Adaptive Deception & Emulation System) and it feeds a hacker not what he needs to know but what he wants to believe. HADES won a 2017 R&D 100 Award presented annually by R&D Magazine.
7. Zero Trust Networks[32] – Zero trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter. No single specific technology is associated with zero trust; it is a holistic approach to network security that incorporates several different principles and technologies.
8. Fileless Malware[33] - Fileless malware refers to a cyberattack technique that uses existing software, allowed applications, and authorized protocols to carry out malicious activities. Fileless malware sneaks in without using traditional executable files as a first level of attack like traditional malware. Rather than using malicious software or downloads of executable files as its primary entry point onto corporate networks, fileless malware often hides in memory or other difficult-to-detect locations. From there, it is written directly to RAM rather than to disk to execute a series of events or is coupled with other attack vectors such as ransomware to accomplish its malicious intent. And because fileless malware doesn't write anything to disk like traditional malware does, it is much harder to detect and may defeat traditional security systems.

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.[34]) 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.

3.4 Recommended Future Assessments

The IDART members have two recommendations for follow-up assessment activities to be conducted by individual entities:

1) Since OASIS nodes are implemented independently, the team recommends conducting internal and external scans of the nodes on a quarterly basis, and a security assessment or penetration

[31] https://www.sandia.gov/news/publications/lab_accomplishments/_assets/documents/lab_accomplish-2010.pdf
[32] https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/
[33] https://www.carbonblack.com/resources/definitions/what-is-fileless-malware/
[34] https://www.dhs.gov/science-and-technology/csd-resources

test. This testing would allow the identification of nodes that are using older/vulnerable versions of software, leak information about the system (ex. list software versions being used) or have vulnerable implementations of their web applications. Since each node can be unique in its software, environment, and supporting security systems, the assessment team recommends that the node owner perform these assessments on their own systems. According to best practices from SANS[35]: "Scans should be performed regularly on all software, services, or platforms (SPPs) that are available external to the organization. At a minimum, scans should be performed monthly."

2) Perform security assessments on applicable software, services or platforms (SSP's). Also according to SANS: "Security assessments should be performed on all externally-accessible SSPs for all new or major application releases. All point releases, patch releases, etc. should be subject to the appropriate level of assessment needed based on the level of risk the change posed to the application but at a minimum, annually." The assessment team recommends that the software vendors, in partnership with their customers, determine the specifics of these assessments to ensure that all relevant risks are addressed.

[35] https://www.sans.org/security-resources/policies/application-security/pdf/web-application-security-policy

4 Appendix A: Adversary Capabilities

This section summarizes the capabilities of various levels of adversary as identified by the Defense Science Board, and Sandia National Laboratories. For more complete information related to these capabilities, see the provided references.

4.1 Defense Science Board Taxonomy of Cyber Security Adversaries

Tier	Description
I	Practitioners who rely on others to develop the malicious code, delivery mechanisms, and execution strategy (use known exploits).
II	Practitioners with a greater depth of experience, with the ability to develop their own tools (from publicly known vulnerabilities).
III	Practitioners who focus on the discovery and use of unknown malicious code, are adept at installing [malware], frequently use data mining tools, target corporate executives and key users (government and industry) for the purpose of stealing personal and corporate data with the expressed purpose of selling the information to other criminal elements.
IV	Criminal or state actors who are organized, highly technical, proficient, well-funded professionals working in teams to discover new vulnerabilities and develop exploits.
V	State actors who create vulnerabilities through an active program to "influence" commercial products and services during design, development or manufacturing, or with the ability to impact products while in the supply chain to enable exploitation of networks and systems of interest.
VI	States with the ability to successfully execute full spectrum (cyber capabilities in combination with all of their military and intelligence capabilities) operations to achieve a specific outcome in political, military, economic, etc. domains and apply at scale.

Figure 3: DSB Adversary Capabilities[36]

[36] Defense Science Board, Task Force Report: "Resilient Military Systems and the Advanced Cyber Threat", January 2013, Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics.

4.2 Generic Threat Matrix

THREAT LEVEL	THREAT PROFILE						
	COMMITMENT			RESOURCES			
					KNOWLEDGE		
	INTENSITY	STEALTH	TIME	TECHNICAL PERSONNEL	CYBER	KINETIC	ACCESS
1	H	H	Years to Decades	Hundreds	H	H	H
2	H	H	Years to Decades	Tens of Tens	M	H	M
3	H	H	Months to Years	Tens of Tens	H	M	M
4	M	H	Weeks to Months	Tens	H	M	M
5	H	M	Weeks to Months	Tens	M	M	M
6	M	M	Weeks to Months	Ones	M	M	L
7	M	M	Months to Years	Tens	L	L	L
8	L	L	Days to Weeks	Ones	L	L	L

Figure 4: Generic Threat Matrix[37]

[37] Duggan, David P. et al. "Categorizing threat: Building and using a generic threat matrix." *Sandia National Laboratories report SAND2007-5791, Albuquerque, New Mexico* (2007).

Appendix B: Attack Graphs

This section contains sample attack graphs for an attack against the gas market. These graphs illustrate the complexity of the system, and how difficult it would be to disrupt operations from the business side of the network. However, it should be noted that utilizing backup procedures, as noted in the Business Operations report that was delivered along with this Addendum Report, will have a performance, efficiency, and economic impact; but will not cause a failure in operations.

The attack graphs illustrate all the steps an attacker must take to move from their access point in the system and move to the consequence of concern. In this case, the access point is a compromise of the business network. For example, as with the Ukrainian Power Grid Attack, this could be done with a successful phishing email campaign. This starting point also assumes that the attacker is not able to pivot into the control network and take direct control of the control systems. The consequence of concern is the misrouting of gas, including failure to appropriately deliver gas. Any malicious activity that allows the unexpected or undetected transfer of – or the failure to transfer – gas would meet this criterion.

B.1 Attack Graph for a Single Organization

The diagram below (Figure 5) illustrates the attack path against a single organization that is involved in the transfer of gas. It illustrates the number of steps it would take to compromise all of the independent systems (as described in Section 2.1.2), including hiding the activity from the humans monitoring operations in order to misroute gas for a single organization.

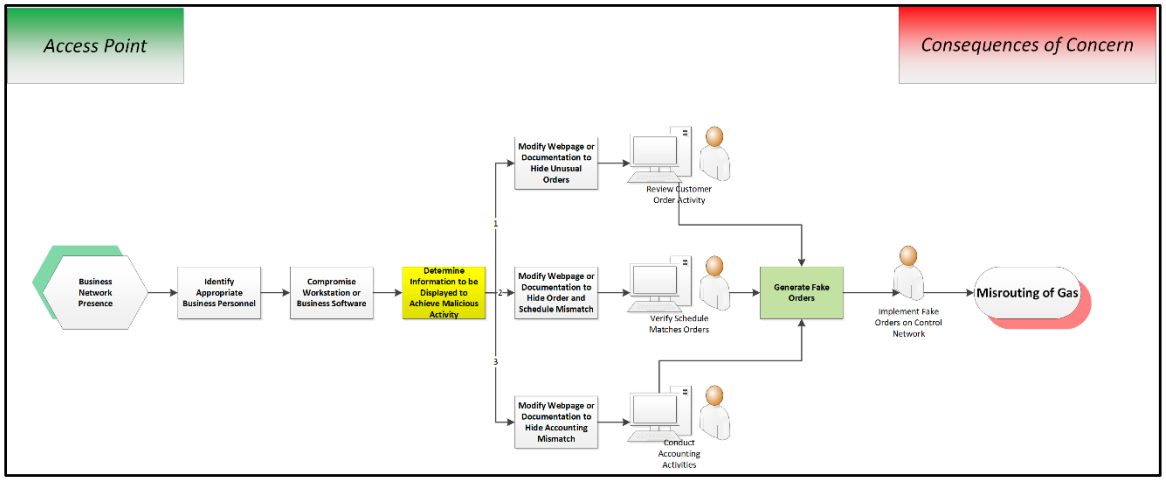

Figure 5: Attack Path Against a Single Organization

In the attack path, we see that an attacker must identify the appropriate business personnel, their workstations, and the applications that are being used. Since current operations utilize “humans in the loop”, an attacker must manipulate the workstations and applications to ensure they do not detect the malicious activity. Once the attacker has completed these steps, they must ensure that the three labeled attack paths are executed in parallel. If they do not manage to conduct all three in parallel, one of the human operators will detect a problem and act to prevent the malicious activity.

If the attacker can prevent the various users from detecting the malicious activity, then the system will generate the malicious orders. There is a chance that the control system personnel will notice any issues or deviations from normal operations but, if they do not detect this change, then gas is misrouted according to the adversary's goals.

B.2 Attack Path Description for Multiple Organizations

The previous attack illustrated the complexity of attacking a single organization. However, since the upstream and downstream values for gas transport must also match, we must extend this attack to multiple organizations. As can be seen in Figure 6, for this attack to be carried out, the attacker must be able to synchronize the attack against multiple organizations. This includes any modifications that are made at a single organization that needs to be propagated to all affected organizations.

Added to the attack path is also the step that stealth must be maintained across all organizations affected. If malicious behavior is detected at any one of the organization, the assessment team assumes that organization will move to notify all of its partners of the malicious activity to ensure the restoration of normal, and expected, operations.

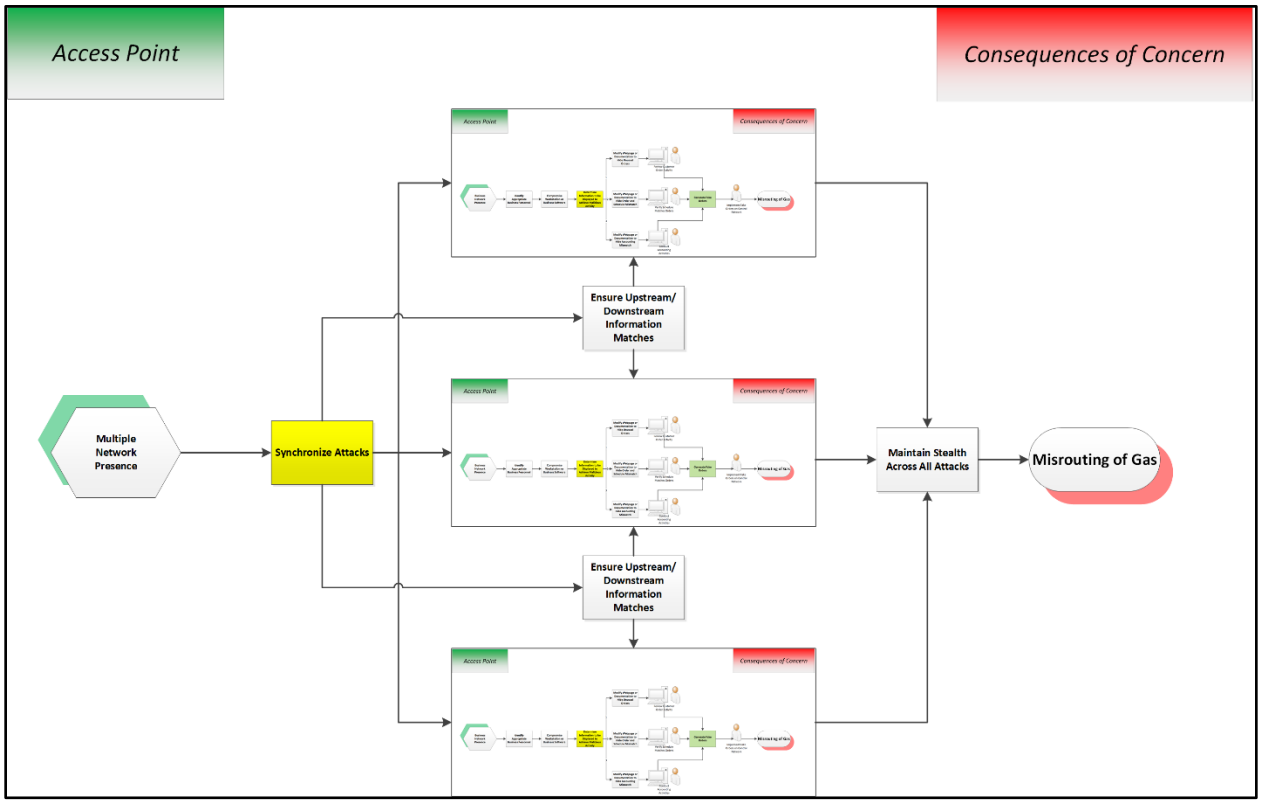

Figure 6: Attack Path Against Multiple Organizations

B.3 Difficulty of Conducting a Cyber Attack

While all the components for a successful attack – compromising a business network, modifying the display of information in a user's browser or application, and compromising accounting applications – have been demonstrated against other industries in the past, many of these attacks require advanced adversaries; especially given the level of coordination needed to avoid detection. Given the resources available to high-level adversaries (such as the resources to bribe personnel), the assessment team feels that these organizations would seek alternative methods to achieve their goals.

Appendix C – Federal Cyber Incident Organizations

Existing federal roles and responsibilities. The following summarizes relevant government organizations, their roles, requirements and contact mechanisms:

- Federal Bureau of Investigation (FBI)
  - FBI Field Office Cyber Task Forces: http://www.fbi.gov/contact-us/field
  - Internet Crime Complaint Center (IC3): http://www.ic3.gov

  Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to FBI Field Office Cyber Task Forces.

  Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties.
- National Cyber Investigative Joint Task Force
  - NCIJTF CyWatch 24/7 Command Center: (855) 292-3937 or cywatch@ic.fbi.gov

  Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of federal law enforcement agencies or the Federal Government.
- United States Secret Service
  - Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs): http://www.secretservice.gov/contact/field-offices

  Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information.
- United States Immigration and Customs Enforcement / Homeland Security Investigations (ICE/HSI)
  - HSI Tip Line: 866-DHS-2-ICE (866-347-2423) or https://www.ice.gov/webform/hsi-tip-form
  - HSI Field Offices: https://www.ice.gov/contact/hsi
  - HSI Cyber Crimes Center: https://www.ice.gov/cyber-crimes

  Report cyber-enabled crime, including: digital theft of intellectual property; illicit e-commerce (including hidden marketplaces); Internet-facilitated proliferation of arms and strategic technology; child pornography; and cyber-enabled smuggling and money laundering.