**TO:** All Interested Parties

**FROM:** Board CIC Chair and Vice Chair

**RE: Proposed Surety Assessment Standard Development Activities and Assignments Work Paper – Addendum Report**

Proposed Surety Assessment Standard Development Activities and Assignments – Addendum Report – DRAFT

On July 22, 2019, Sandia National Laboratories provided NAESB with the final reports on the surety assessment: (1) Assessment Report of the NAESB Public Key Infrastructure Program; (2) Assessment Report of the NAESB OASIS Standards; (3) Assessment Report of the NAESB Business Operations Practices and Standards; and (4) Addendum Report: Threat-based Examination of NAESB Standards and Business Operations. In anticipation of these reports being delivered, NAESB included on its 2019 Annual Plans a review of the final reports and the development and/or modifications of NAESB Business Practice Standards as needed to address recommendations from Sandia National Laboratories. The Department of Energy has requested that, where possible, NAESB expediate any resulting standard development. To assist in these efforts, the Critical Infrastructure Committee has committed to reviewing the final reports to provide context to any recommendations containing actionable items for standards development.

**Additional Findings and Considerations**

This work paper identifies the additional findings and considerations identified by Sandia National Laboratories in the Addendum Report: Threat-based Examination of NAESB Standards and Business Operations and the related standard development activities identified by the Board Critical Infrastructure Committee that NAESB may want to consider in response. As part of this report, Sandia National Laboratories identifies ten considerations across six different sections: Section 2.3.1 EDI Cyber Attack, Section 2.3.2 Ukrainian Power Grid Attack, Section 3.1 Trends in Operation, Section 3.2 Government and Industry Standards, Section 3.3 Emerging Technologies, and Section 3.4 Recommended Future Assessments.

The table below captures the ten findings and the related standard considerations to potentially incorporate the identified concept into the standards, as applicable.

| **Issue** | **Report Section (Page Number)** | **Sandia Finding or Consideration** | **Standards Considerations (if applicable)** | **Assignment (if applicable)** |
| --- | --- | --- | --- | --- |
| 1. | Addendum Report Section 2.3.1 – EDI Cyber Attack (Pages 21 – 23) | 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. | This is not currently a requirement of the NAESB standards nor is this a function currently provided by NAESB  Industry may want to consider if there is a benefit to individual entities tracking information identified by the metrics. | N/A |
| 2. | Addendum Report Section 2.3.1 – EDI Cyber Attack (Pages 21 – 23) | 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*.  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. | This is not currently a requirement of the NAESB standards nor is this a function currently provided by NAESB.  Coordination with other organizations is a function of the NAESB Board of Directors | N/A |
| 3. | Addendum Report Section 2.3.1 – EDI Cyber Attack (Pages 21 – 23) | 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…  These reports can take the shape of a wizard driven reporting mechanism that populates a database such as the US CERT[[1]](#footnote-1), DHS[[2]](#footnote-2) and DOE[[3]](#footnote-3) 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. | This is not currently a requirement of the NAESB standards nor is this a function currently provided by NAESB.  Coordination with other organizations is a function of the NAESB Board of Directors | N/A |
| 4. | Addendum Report Section 2.3.2 – Ukrainian Power Grid Attack (Pages 23 – 25) | 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. | The WGQ EDM Manual requires HTTP Basic Authentication or similar logon/password mechanisms for customer activity websites (WGQ 4.3.60) and accessing Interactive Flat File EDM (WGQ 4.3.84)  The RMQ EDM Manual relies on the RMQ IET Standards for security principles, including authentication. (RXQ.5.6 Technical Implementation)  The WGQ/RMQ IET Standards require basic authentication (WGQ.10.3.16 and RMQ.7.3.16) with the Security Sections (WGQ Page 20 and RMQ Page 14) specifically requiring 128-bit SSL-protected usernames and passwords to establish authentication and list optional techniques such as firewall security for further authentication.  The WEQ-012.1.9 allows for the issuance of digital certificates for (1) individual subscribers; (2) role; (3) device; and (4) application  WEQ-002-3.1(b) requires each user requesting access to OASIS to provide a digital certificate issued by an ACA that will be used by the user in accessing OASIS  WEQ-004-2.3 states that e-Tag communications and services implemented using the e-Tag Spec shall be secured using a certificate issued by an ACA  WEQ-022-1.2 requires a certificate issued by an ACA for each user accessing the NAESB EIR | WGQ EDM Subcommittee and RMQ IR/TEIS  WEQ Cybersecurity Subcommittee  WEQ OASIS Subcommittee  WEQ CISS  WEQ CISS |
| 5. | Addendum Report Section 2.3.2 – Ukrainian Power Grid Attack (Pages 23 – 25) | 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:   * 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? | N/A | N/A |
| 6. | Addendum Report Section 3.1 – Trends in Operation (Pages 26 – 27) | 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 have a method to disconnect the equipment from the control network and conduct manual operations until normal operations can be restored. |  |  |
| 7. | Addendum Report Section 3.2 – Government and Industry Standards (Page 27) | 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.[[4]](#footnote-4) 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.[[5]](#footnote-5)  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[[6]](#footnote-6) * NISTIR 8144 (DRAFT): Assessing Threats to Mobile Devices and Infrastructure - The Mobile Threat Catalog[[7]](#footnote-7) * NCCoE Project: Mobile Device Security: Cloud and Hybrid Builds[[8]](#footnote-8) | N/A  Review of this recommendation will be considered if/when NAESB develops standards in this area. | N/A |
| 8. | Addendum Report Section 3.3 – Emerging Technologies (Pages 27 – 29) | 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)[[9]](#footnote-9). 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.  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.[[10]](#footnote-10)  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) technology and a supercomputing cluster to watch how botnets work and explore ways to stop them.[[11]](#footnote-11)  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.  Zero Trust Networks[[12]](#footnote-12) – 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.  Fileless Malware[[13]](#footnote-13) - 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. | N/A  Review of this recommendation will be considered if/when NAESB develops standards in this area. | N/A |
| 9. | Addendum Report Section 3.4 – Recommended Future Assessments (Pages 29 – 30) | 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 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[[14]](#footnote-14): “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.” | N/A |  |
| 10. | Addendum Report Section 3.4 – Recommended Future Assessments (Pages 29 – 30) | 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. | N/A |  |

1. US-CERT Incident Reporting System, <https://www.us-cert.gov/forms/report> [↑](#footnote-ref-1)
2. Report Cyber Incidents, <https://www.dhs.gov/how-do-i/report-cyber-incidents> [↑](#footnote-ref-2)
3. DOE - JC3 Incident Reporting, <https://tickets.ijc3.doe.gov> [↑](#footnote-ref-3)
4. <https://www.nist.gov/itl/nist-cloud-computing-related-publications> [↑](#footnote-ref-4)
5. <https://www.nist.gov/topics/internet-things-iot> [↑](#footnote-ref-5)
6. <https://csrc.nist.gov/publications/detail/sp/800-124/rev-1/final> [↑](#footnote-ref-6)
7. <https://www.nccoe.nist.gov/sites/default/files/library/mtc-nistir-8144-draft.pdf> [↑](#footnote-ref-7)
8. <https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/cloud-hybrid> [↑](#footnote-ref-8)
9. <https://www.sandia.gov/emulytics/> [↑](#footnote-ref-9)
10. <https://www.sandia.gov/news/publications/lab_accomplishments/articles/2018/adv_science_and_tech.html> [↑](#footnote-ref-10)
11. <https://www.sandia.gov/news/publications/lab_accomplishments/_assets/documents/lab_accomplish-2010.pdf> [↑](#footnote-ref-11)
12. <https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/> [↑](#footnote-ref-12)
13. <https://www.carbonblack.com/resources/definitions/what-is-fileless-malware/> [↑](#footnote-ref-13)
14. <https://www.sans.org/security-resources/policies/application-security/pdf/web-application-security-policy> [↑](#footnote-ref-14)