**TO:** All Interested Parties

**FROM:** Board Critical Infrastructure Committee

**RE: Surety Assessment Standard Development Activities and Assignments**

Surety Assessment Assignments to Board Digital Committee

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 committed to reviewing the final reports to provide context to any recommendations containing actionable items for standards development.

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

*Additional Findings and Considerations*

As part of the Addendum Report: Threat-based Examination of NAESB Standards and Business Operations, the Critical Infrastructure Committee identified two areas as part of the additional findings or considerations made by Sandia National Laboratories for consideration by the Digital Committee. These two findings or considerations were made by Sandia National Laboratories as part of Section 3.2 and 3.3 of the report. These sections address future trends in operations and technical areas that are expected to be adopted in the future.

| **Issue** | **Report Section (Page Number)** | **Sandia Finding or Consideration** | **Standards Consideration (if applicable)** | **Assignment (if applicable)** |
| --- | --- | --- | --- | --- |
| 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.[[1]](#footnote-1) 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.[[2]](#footnote-2)  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[[3]](#footnote-3) * NISTIR 8144 (DRAFT): Assessing Threats to Mobile Devices and Infrastructure - The Mobile Threat Catalog[[4]](#footnote-4) * NCCoE Project: Mobile Device Security: Cloud and Hybrid Builds[[5]](#footnote-5) | N/A  Review of this recommendation will be considered if/when NAESB develops standards in this area. | Board Digital Committee |
| 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)[[6]](#footnote-6). 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.[[7]](#footnote-7)  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.[[8]](#footnote-8)  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[[9]](#footnote-9) – 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[[10]](#footnote-10) - 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. | Board Digital Committee |

1. <https://www.nist.gov/itl/nist-cloud-computing-related-publications> [↑](#footnote-ref-1)
2. <https://www.nist.gov/topics/internet-things-iot> [↑](#footnote-ref-2)
3. <https://csrc.nist.gov/publications/detail/sp/800-124/rev-1/final> [↑](#footnote-ref-3)
4. <https://www.nccoe.nist.gov/sites/default/files/library/mtc-nistir-8144-draft.pdf> [↑](#footnote-ref-4)
5. <https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/cloud-hybrid> [↑](#footnote-ref-5)
6. <https://www.sandia.gov/emulytics/> [↑](#footnote-ref-6)
7. <https://www.sandia.gov/news/publications/lab_accomplishments/articles/2018/adv_science_and_tech.html> [↑](#footnote-ref-7)
8. <https://www.sandia.gov/news/publications/lab_accomplishments/_assets/documents/lab_accomplish-2010.pdf> [↑](#footnote-ref-8)
9. <https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/> [↑](#footnote-ref-9)
10. <https://www.carbonblack.com/resources/definitions/what-is-fileless-malware/> [↑](#footnote-ref-10)