**TO:** All Interested Parties

**FROM:** Caroline Trum, NAESB Deputy Director

**RE: Proposed Surety Assessment Standard Development Activities and Assignments Work Paper – NAESB Business Operations Practices and Standards**

Proposed Surety Assessment Standard Development Activities and Assignments – NAESB Business Operations Practices and Standards

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. The table below identifies the explicit findings and other recommendations in the Assessment Report of the NAESB Business Operations Practices and Standards and the corresponding standard development activities to address the recommendations from Sandia National Laboratories.

| **Issue** | **Report Section (Page Number)** | **Sandia Finding/Recommendation** | **Recommended Standards Development Activity** | **Recommended Assignment** |
| --- | --- | --- | --- | --- |
|  | Business Operations Practices and Standards Report Section 4 – Metrics of Importance (Pages 8 – 9) | Metrics should be collected and analyzed to measure how the implementation of the Business Operations Practices and Standards increases the reliability and security of electronic data exchanged between trading partners. The following are some examples of metrics that could be collected for NAESB and industry partners to review and analyze:* Measure the number of daily transactions between business partners, and the number of transactions that fail or have errors that need to be corrected
* Measure the best, median, average, and worst time for a transaction to be completed
* Count the number of organizations that have established continuity of operations planning (COOP), and the number of organizations that exercise their COOP each year
* Count the number of organizations that maintain alternate and 24/7 contact information for trading partners, and the number that have this information stored offline (in case of a ransomware attack)
* Count the number of times alternate methods were used for transactions (ex. phone or fax) during normal operations; and during a system outage, failure, or other issue

These metrics could be self-reported – either to NAESB or maintained by each organization on a statistics webpage that can be accessed by their trading partners. If desired, NAESB could collect and tabulate the totals on a monthly basis, and then share the information with participating organizations. If necessary, data could be anonymized while still allowing organizations to rate their own performance against the industry norms.This data could then be used in life-cycle decisions, trading partner selection, analysis of COOP and disaster recovery plans, and determining if NAESB standards need to be upgraded or revised. |  |  |
|  | Business Operations Practices and Standards Report Section 6.1.1 – NAESB Standards Refer to Vulnerable Versions of Communication Protocols (Page 10 – 11) | Level: HighIn addition, to ensure timely adoption of new technology the assessment team recommends that new versions of technologies and standards that include fixes or patches for known vulnerabilities (as opposed to simply adding new functionality) should be adopted within 30 days of their publication. |  |  |
|  | Business Operations Practices and Standards Report Section 6.1.1 – NAESB Standards Refer to Vulnerable Versions of Communication Protocols (Pages 10 – 11) | Level: HighSince existing systems may not be compatible with updated software packages or protocol versions, updates may be too expensive to utilize, or for other business related decisions, the assessment team recommends the owning organization notify their trading partners of any systems or software that have not been updated and the potential impact of utilizing the vulnerable system in the 30-day window. This allows business partners to assess the risk of conducting business over those legacy systems. |  |  |
|  | Business Operations Practices and Standards Report Section 6.1.1 – NAESB Standards Refer to Vulnerable Versions of Communication Protocols (Pages 10 – 11) | Level: HighAll the communications standards specified in the Internet Electronic Transport (IET) standards and the Electronic Delivery Manual (EDM) for Retail Gas Quadrant and Retail Electric Quadrants. The assessment team recommends that the NAESB review and upgrade the minimum requirement for SSL/TLS to version 1.2 configured with FIPS-based cipher suites as a minimum[[1]](#footnote-1). NIST 800-52 details the TLS version and associated configurations and currently requires version 1.2 and support for version 1.3 by January 1, 2021. Specific configurations for TLS servers and TLS versions are detailed in section 4 of NIST 800-52 and the specific server implementation is dependent on the TLS version and implementation strategy. SSL protocol is disallowed for both government and business – facing applications and as such, the assessment team recommends disallowing support for SSL version protocols.  |  |  |
|  | Business Operations Practices and Standards Report Section 6.1.1 – NAESB Standards Refer to Vulnerable Versions of Communication Protocols (Pages 10 – 11) | Level: HighIn addition, while implementation details are outside the purview of NAESB, the assessment team recommends adding a note that any major security bulletins or recommendations should, at the least, be considered for implementation within a 30-day window, even if a new version of the standard is not yet available or finalized. |  |  |
|  | Business Operations Practices and Standards Report Section 6.1.2 – NAESB Standards Need Review for Unused or Unnecessary Functionality (Page 11) | Level: LowAs part of an annual review the analysis team recommends review of NIST 800-52 for guidance. Monitoring of required protocols as defined in WEQ-002.3 and the IET data dictionary tableupdates for acceptable configurations for supported secure communication protocols defined for IET are all recommended for immediate update as required by independent facility implementation based on NIST NVD, US CERT, ICS CERT or vendor mandate. The assessment team recommends any updates for these communication protocols to be considered for incorporation into standards following review as an updated minimum version as included in the Wholesale Gas Electronic Delivery Mechanism Related Standards and incorporated by FERC in 18 CFR 284.12 updating to the latest versions of available protocols as soon as practicable and not to exceed 9 months is a general best practice that organizations within the wholesale electric quadrant, retail electric and retail gas quadrants should consider for incorporation as well. |   |  |
|  | Business Operations Practices and Standards Report Section 6.1.4 – Use of Human Control and Review in Operations (Page 12) | Level: N/AWith the current trend towards more automation and computer control, this strength should be considered when replacing human operators with autonomous systems. Many tools exist to help automate both security of network systems and can provide additional support for monitoring network traffic and operations through technologies such as Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), machine learning, user behavioral analysis, zero trust models or other technologies that may become available. These are implementation details that may optionally be reviewed for acceptable standards.[[2]](#footnote-2) This includes recommended guidelines for configuration and even logging, network traffic monitoring, and alerting systems. The assessment team also recommends that, at a minimum, humans retain monitoring capability and where possible provide manual continuity of operations in the event of abnormal behavior or failure conditions with the system. |  |  |
|  | Business Operations Practices and Standards Report Section 6.1.5 – Separation of Business and Control Computer Networks (Page 12 – 13) | Level: N/ASome commonly suggested security solutions are to isolate the SCADA and PCN systems from the Internet and corporate enterprise network (EN) through the use of firewalls, which can be complex devices to design and deploy correctly, data diode separation which allows network data to flow in one direction allowing for monitoring of control systems but not allowing control signals to traverse from the business side network to the control network, virtual private network implementation which restricts access to designated portions of the network, internet protocol security (IP sec) which is a protocol implementation designed to require encryption between two devices and requires a shared public key. This Centre for the Protection of National Infrastructure (CPNI) Good Practice document addresses the need for guidance in creating such firewalls. There are a significant number of different solutions used by the industry and the security effectiveness of these can vary widely. In general, architectures that allow the establishment of a Demilitarized Zone (DMZ) between the enterprise network and SCADA/PCN network will provide the most effective security solution. Realize this part of defense-in-depth strategy. Here is more complete treatment [[3]](#footnote-3)Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, Industrial Control Systems Cyber Emergency Response Team, September 2016.  |  |  |
|  | Business Operations Practices and Standards Report – Section 6.1.6 Continued Use of Different Security Paradigms (Pages 13 – 15) | Level: N/ABoth PGP and PKI provide adequate security provided they are properly configured and NIST - 131A encryption and decryptions denotes AES encryption and decryption as acceptable. NIST - 131A makes allowance for some legacy encryption and decryption algorithms, the assessment team recommends removal of legacy support and a minimum encryption strength of 128 bits. This is consistent with NAESB Internet Electronic Transport standards which requires 128-bit strength encryption. |  |  |
|  | Business Operations Practices and Standards Report – Section 6.1.6 Continued Use of Different Security Paradigms (Pages 13 – 15) | Level: N/AThe assessment team recommends that updates within the IET standards to clarify language under the security section to NIST 800-52 details the TLS version and associated configurations and currently requires version 1.2 and support for version 1.3 by January 1, 2021. Specific configurations for TLS servers and TLS versions are detailed in section 4 of NIST 800-52 and the specific server implementation is dependent on the TLS version and implementation strategy. NIST 800-52 disallows SSL implementation for both government and business – facing applications and as such, the assessment team recommends disallowing support for SSL version protocols and implement TLS version 1.2 as described. |  |  |
|  | Business Operations Practices and Standards Report – Section 6.1.6 Continued Use of Different Security Paradigms (Pages 13 – 15) | Level: N/AAn HTTPS[[4]](#footnote-4) solution will protect information in transit, supporting overall privacy needs. Using basic authentication over HTTP is inherently insecure as username/password combinations are not encrypted in HTTP basic authentication[[5]](#footnote-5). If the communication channel is secured via HTTPS, then those credentials are secured as well. While self-signed certificates are acceptable for payload protection, HTTPS communication must be secured via certificates issued by a trusted, commercial certificate authority such as a NAESB ACA in order to verify certificate authenticity. Additional options for certificate authorities include commercial certificate authorities include IdenTrust, Comodo, GoDaddy, GlobalSign, and DigiCert; other valid certificate authorities exist as well. |  |  |
|  | Business Operations Practices and Standards Report – Section 6.1.6 Continued Use of Different Security Paradigms (Pages 13 – 15) | Level: N/AKey lengths must be updated to reflect current acceptable encryption strength[[6]](#footnote-6). Specifically, RSA keys must be no shorter than 2048 bits, while ECDSA keys must be no shorter than 224 bits. Hash algorithms should be from the SHA-2 or SHA-3 families. Acceptable AES key lengths range from 128, to 192, to 256. In general, implementors should use the largest feasible key length consistent with implementation of current business processes. In order to be in compliance with these stronger algorithms, any PGP command line clients should be at version 9 or greater as earlier versions did not support SHA-2 or SHA-3 family hashing algorithms or fully support AES[[7]](#footnote-7). |  |  |
|  | Business Operations Practices and Standards Report – Section 6.1.6 Continued Use of Different Security Paradigms (Pages 13 – 15) | Level: N/AFinally, IET business process as currently implemented may be vulnerable to both replay[[8]](#footnote-8) and amplification[[9]](#footnote-9) attacks. Based on the assessment teams review of the transactional process these two attacks were immediately identified as attacks of concern…Note that this attack is feasible even with payloads that are encrypted with foreign, untrusted keys, or with payloads that are filled with garbage bits. Two basic approaches exist to help eliminate this kind of amplification attack. The first strategy involves making error notification messages to be as small as possible and smaller than the original requests. This way, an attacker using this mechanism will not be able to amplify the volume of data sent to a target; rather, as the response message is smaller, the overall denial-of-service risk will be correspondingly lowered. The second strategy uses rate limiting to ensure that error messages are sent at a rate that is lower than expected message processing speeds. This way, even if the responses are larger than the adversary-submitted requests, they will not be sent to the target at a rate that would strain target computational resources.  |  |  |

1. NIST 800-52 section 3.1 Protocol Version Support <https://csrc.nist.gov/CSRC/media/Publications/sp/800-52/rev-2/draft/documents/sp800-52r2-draft2.pdf> [↑](#footnote-ref-1)
2. NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS) <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf> [↑](#footnote-ref-2)
3. (<https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf>) [↑](#footnote-ref-3)
4. *Securing the Web*, retrieved on June 10, 2019, from <https://www.w3.org/2001/tag/doc/web-https> [↑](#footnote-ref-4)
5. RFC 2617: *HTTP Authentication: Basic and Digest Access Authentication*, retrieved on June 10, 2019, from <https://tools.ietf.org/html/rfc2617> [↑](#footnote-ref-5)
6. Barker, E. and Roginsky, A. NIST 800-131A: *Transitioning the Use of Cryptographic Algorithms and Key Lengths*. National Institute of Standards and Technology, 2019. [↑](#footnote-ref-6)
7. Symantec Corporation. *PGP Command Line 9.0 User’s Guide*. Symantec, 2006. [↑](#footnote-ref-7)
8. *Replay Attacks*, retrieved on June 10, 2019, from <https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/replay-attacks> [↑](#footnote-ref-8)
9. *DNS Amplification Attacks*, retrieved on June 10, 2019, from <https://www.us-cert.gov/ncas/alerts/TA13-088A> [↑](#footnote-ref-9)