WEQ Cybersecurity Subcommittee Assignments

**Assessment Report of the NAESB Business Operations Practices and Standards**

Additional Findings and Considerations

This section of this work paper identifies additional findings and considerations identified by Sandia National Laboratories as part of Section 4 Metrics of Importance and Section 6.2 Strengths of the NAESB Business Operations Practices and Standards of the Assessment Report of the NAESB Business Operations Practices and Standards and the related standard development activities identified by the Board Critical Infrastructure Committee that NAESB may want to consider in response. As indicated by Sandia National Laboratories, these two sections of the report specifically address metrics and “areas the assessment team identified as practices or requirements that prevented or increased the difficulty of a successful attack or exploitation by an adversary. Within Section 4 Metrics, there is one area of consideration. As part of Section 6.2 Strengths of the NAESB Business Operations Practices and Standards, there are three areas of consideration: Section 6.2.1 Use of Human control and Review of Operations, Section 6.2.2 Separation of Business and Control Computer Networks, and Section 6.2.3 Gas and Electric Industry Interactions. In total, there are eight findings or considerations from Sandia National Laboratories.

The table below captures the eight findings and the related standard considerations to potentially incorporate the identified concept into the standards, as applicable, assigned to the WEQ Cybersecurity Subcommittee.

| **Issue** | **Report Section (Page Number)** | **Sandia Finding or Consideration** | **Standard Considerations (if applicable)** | **Assignment (if applicable)** |
| --- | --- | --- | --- | --- |
| 7. | Business Operations Practices and Standards Report Section 6.1.4 – Use of Human Control and Review in Operations (Page 12)(Table of Contents Section 6.2.1 Use of Human Control and Review in Operations) | With 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.[[1]](#footnote-1) 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. | Subcommittees should consider standard(s) to address recommended guidelines for configuration and logging, network traffic monitoring, and alerting systems as well standard(s) requiring manual continuity of operations in the event of abnormal behavior or failure conditions with the system. | WEQ Cybersecurity Subcommittee should investigate applicability to WEQ Business Practice StandardsThis could have potential applicability to OASIS and e-Tagging but needs additional discussion. This discussion will likely need to include input from other subcommittees and WEQ EC.This may take substantial effort to address through standards development.The WGQ EDM Subcommittee and RMQ IR/TEIS modified the standards and model business practices to include both specific and broad adoption of system security measures as well as specific notifications and coordination during outages with effected trading partners. These changes were incorporated as part of the new WGQ Standard Nos. 4.3.109 and 10.3.28 and new RMQ Model Business Practice No. 7.3.28.6/29/20 – The WEQ OASIS and WEQ CISS have discussed this issue. Joint meetings may be necessary to further discussions. |
| 13. | Business Operations Practices and Standards Report – Section 6.1.6 Continued Use of Different Security Paradigms (Pages 13 – 15)(Table of Contents Section 6.2.3 Gas and Electric Industry Interactions) | Finally, IET business process as currently implemented may be vulnerable to both replay[[2]](#footnote-2) and amplification[[3]](#footnote-3) 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.  | The subcommittees should consider standard(s) to address mitigation of replay and amplification attacks as aligned with recommended strategies | WEQ Cybersecurity SubcommitteeThis issue may take a substantial effort to address through standards development. Work should be done to coordinate with the WGQ and RMQ and address in a similar manner.6/29/20 – The WEQ OASIS and WEQ CISS have discussed this issue. Joint meetings may be necessary to further discussions. |

1. NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS) <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf> [↑](#footnote-ref-1)
2. *Replay Attacks*, retrieved on June 10, 2019, from <https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/replay-attacks> [↑](#footnote-ref-2)
3. *DNS Amplification Attacks*, retrieved on June 10, 2019, from <https://www.us-cert.gov/ncas/alerts/TA13-088A> [↑](#footnote-ref-3)