**1. RECOMMENDED ACTION: EFFECT OF EC VOTE TO ACCEPT RECOMMENDED ACTION:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Accept as requested |  | Change to Existing Practice |
|  | Accept as modified below | x | Status Quo |
| x | Decline |  |  |

**2. TYPE OF DEVELOPMENT/MAINTENANCE**

|  |  |
| --- | --- |
| **Per Request:** | **Per Recommendation:** |
|  | Initiation |  | Initiation |
| x | Modification |   | Modification |
|  | Interpretation |  | Interpretation |
|  | Withdrawal |  | Withdrawal |
|  |  |  |  |
|  | Principle |  | Principle |
|  | Definition |  | Definition |
| x | Business Practice Standard |  | Business Practice Standard |
| x | Document |  | Document |
|  | Data Element |  | Data Element |
|  | Code Value |  | Code Value |
|  | X12 Implementation Guide |  | X12 Implementation Guide |
|  | Business Process Documentation |  | Business Process Documentation |

**3. RECOMMENDATION**

**SUMMARY:**

No further action is necessary at this time.

**4. SUPPORTING DOCUMENTATION**

**a. Description of Request:**

2020 WEQ Annual Plan Item 6.a – Develop and/or modify the NAESB Business Practice Standards as needed to address the Additional Findings and Considerations identified by Sandia National Laboratories

**b. Description of Recommendation:**

No action is recommended at this time. Following recommendations developed in 2019 to address the recommendations from Sandia National Laboratories, there were two additional findings assigned to the WEQ to be addressed:

| **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 Standards |
| 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 Subcommittee |

**c. Business Purpose:**

The subcommittee determined that no further action is needed at this time. These issues are either adequately addressed through requirements found in WEQ-001-8, WEQ-002-5, the NAESB Accreditation Requirements for Authorized Certification Authorities or the Board Certification Committee ACA Process or not applicable to the processes and communication protocols utilized by the WEQ.

**d. Commentary/Rationale of Subcommittee(s)/Task Force(s):**

Reference WEQ CSS Meeting Minutes:

* [May 12, 2020](https://naesb.org/pdf4/weq_css051220fm.doc)
* [June 30, 2020](https://naesb.org/pdf4/weq_css063020fm.doc)
* [August 11, 2020](https://www.naesb.org/pdf4/weq_css081120fm.doc)
* August 25, 2020

 Reference joint WEQ CSS and WEQ OASIS Subcommittee Meeting Minutes:

* August 4, 2020
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)