**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:**

Review WEQ Standards for impact of XML vulnerability exploits and make modifications as needed to standards and functional specifications

**Recommended Standards:**

No new standard development or changes to existing standards/functional specifications are proposed.

**4. SUPPORTING DOCUMENTATION**

**a. Description of Request:**

2015 WEQ Annual Plan Item 4.b – Review WEQ standards for impact of XML vulnerability exploits and make modifications as needed to standards and functional specifications

**b. Description of Recommendation:**

The WEQ Cybersecurity Subcommittee and Coordinate Interchange Scheduling Subcommittee are jointly recommending that no action be taken on 2015 WEQ Annual Plan Item 4.b.

**c. Business Purpose:**

There is no business purpose to modify any standard or functional specification as no known XML vulnerabilities impact the WEQ Business Practice Standards or functional specifications.

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

The subcommittees met jointly to discuss the issue and determined that no XML vulnerability currently exists which impacts the standards and/or functional specifications and needs to be addressed. Therefore, the subcommittees voted jointly on the no action recommendation. Please see the meeting minutes from joint meeting on April 29, 2015.

Additionally, the Cybersecurity Subcommittee met on July 13, 2015 to review an XML vulnerability brought to its attention following the April 29, 2015 joint meeting and determined that the vulnerability did not pose a risk to NAESB Business Practice Standards of Functional Specifications and agreed it was appropriate to proceed with the no action recommendation. Please see the meeting minutes from the meeting on July 13, 2015.