Based on the explicit recommendations and other findings in the surety assessment final reports provided by Sandia National Laboratories to NAESB, the following table identifies the corresponding standard development activities recommended by the Board Critical Infrastructure Committee:

| **Sandia Finding/Recommendation** | **Recommended Standards Development Activity** | **Recommended Subcommittee Assignment** |
| --- | --- | --- |
| PKI Report Section 6.1.1 – Discrepancy between NAESB Standards and Certification Practice Statements:  The ACAs should include verbiage in the CPS that indicates a mismatch between the CPS and NAESB standard will default to the NAESB standard. Alternatively, the CPS could be updated to reference the appropriate NAESB standard(s) instead of including the language directly in the CPS. |  | * WEQ Cybersecurity Subcommittee |
| PKI Report Section 6.1.2 – Possible Incomplete Enforcement of NAESB Standards Assurance Levels  Investigate if “High” assurance level certificates have been issued and review if there needs to be changes to the retention period in either the NAESB standard, or in the GlobalSign CPS. (Note: Section 4.4 Records Retention Policy of the OATI CPS indicates records will be retained for “time periods required by applicable standards”.) |  | * WEQ Cybersecurity Subcommittee |
| OASIS Report Section 6.1.1 – Significant Amounts of Sensitive Information are Posted on OASIS  Continue to leverage the NAESB OASIS Subcommittee to ensure there is a balance between protecting sensitive information and meeting industry needs. In addition, the assessment team recommends that NAESB work with their partners and FERC to determine if more stringent security testing – similar to that used for ACAs – is desirable for OASIS Node operators to ensure the nodes are secure from cyber attacks. |  | * WEQ OASIS Subcommittee |
| OASIS Report Section 6.1.2 – Implementation Details for OASIS Nodes Unspecified  To mitigate this issue, the assessment team recommends that all OASIS nodes follow industry best practices to secure their systems. This would include, but is not limited to:   * Ensuring web applications are secure against common vulnerabilities such as the OWASP Top 10 * Encrypting all communications (as allowable) * Utilizing the latest versions of all critical standards (such as TLS) * Verifying and validating all external inputs * Conducting business continuity and disaster recovery exercises * Applying patches and updates in a timely manner |  | * WEQ OASIS Subcommittee |
| Business Operations Practices and Standards Report Section 6.1.1 – NAESB Standards Refer to Vulnerable Versions of Communication Protocols  To ensure outdated protocols do not provide a vector for future attacks, the assessment team recommends replacing any reference to a specific version of a technology or protocol with a reference to indicate that the latest version of the technology or protocol should be used. If desirable, a time limit such as “within 30 days of publication” could be added to allow some time for organizations to update their systems and software. In 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 even if a new standard is not yet available |  | * WEQ OASIS Subcommittee * WGQ Electronic Delivery Mechanism Subcommittee * RMQ IR/TEIS Subcommittee |
| Business Operations Practices and Standards Report Section 6.1.2 – NAESB Standards Need Review for Unused or Unnecessary Functionality  To ensure legacy functionality does not provide a vector for future attacks, the assessment team recommends NAESB conduct occasional (ex. annual) reviews of their standards to determine if there is functionality that is defined, but unused, so it can be removed, deprecated or updated. This could be performed by having organizations report what functionality they are currently using, no longer using, or have never used. If utilization of functionality falls below a certain threshold or level of need it could be labeled for deprecation and removal. |  | * WGQ EDM Subcommittee * RMQ IR/TEIS Subcommittee * WEQ OASIS Subcommittee * WEQ CISS |