**Board Certification Program Committee Chairs’ Work Paper – Proposed Surety Assessment Standard Development Activities**

Based on the explicit recommendations and other findings in the surety assessment reports provided by Sandia National Laboratories to NAESB on January 25, 2019, the following table identifies the corresponding standard development activities recommended by the Board Critical Infrastructure Committee:

|  | **Sandia Finding/Recommendation** | **Considerations** | **Proposed Recommended Standards Development Activities** | **Recommended Subcommittee Assignment(s)** |
| --- | --- | --- | --- | --- |
|  | 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. | Should the subcommittee investigate the need for modifications to the NAESB Accreditation Requirements for Certificate Authorities to require a timeline for an ACA’s Certification Practice Statement to be updated following a change to the specification/standards and/or incorporation of a statement regarding conflicts between the specification/standards |  | 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”.) | Should the subcommittee investigate the retention period associated with a High assurance level certificate and, if needed, modify the applicable NAESB Accreditation Requirements for Certification Authorities requirement to make the necessary changes |  | WEQ Cybersecurity Subcommittee |
|  | PKI Report Section 6.3 – Review of X.509 Security  The assessment team recommends organizations that rely on X.509 certificates review their systems and software to determine if they are utilizing technologies that are affected by these vulnerabilities (or any others) and update their systems and software to a version that is not affected. Specific details on individual CVEs can be found in [NIST’s NVD](https://nvd.nist.gov/) along with “References to Advisories, Solutions, and Tools” for each CVE. | Should an evaluation of the vulnerabilities identified in the NIST National Vulnerability Database should be incorporated as part of the WEQ Cybersecurity Subcommittee’s annual evaluation of modifications to the WEQ-012 Public Key Infrastructure and NAESB Accreditation Requirements for Certification Authorities |  | WEQ Cybersecurity Subcommittee |
|  | OASIS Report Section 6.1.1 – Significant Amounts of Sensitive Information are Posted on OASIS  The team recommends that the OASIS Subcommittee consider the sensitivity of historical information and determine what information can be removed on a quarterly basis; however, outside of this consideration, the assessment team does not have any specific recommendations for actions that need to be taken. | Should the subcommittee evaluate if the requirements for data retention on OASIS meet the minimum requirements as mandated by the FERC and determine if the defined maximum period on OASIS should be equal to the FERC mandated minimum or if there is a need for data to be made available for longer periods on OASIS  Should the subcommittee evaluate, for data that may not have a FERC mandated minimum retention period, if a maximum retention period should be defined for making that data available on OASIS |  | 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](https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf) (page 6) * Encrypting all communications (as allowable) using an encryption model that is validated against [FIPS 140-2](https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf) (Validated encryption modules: <https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules>) * Utilizing the latest versions of all critical standards (such as TLS) to ensure all possible vulnerabilities are addressed (addressed under Sandia Finding/Recommendation 6) * Verifying and validating all external inputs * Conducting business continuity and disaster recovery exercises on an annual basis * Applying patches and updates in a timely manner; ideally no longer than 7 days after the patch or update becomes available (if practical) | Should the WEQ OASIS Standards need to be modified incorporate mitigation of application security risks identified in the OWASP Top 10   * If so, does the information/resources included by Sandia provide enough detail regarding mitigation to identify specific standard modifications   Should the WEQ OASIS Standards be reviewed to identify any unencrypted data communications and then modified to recommend an encryption method for those data communications   * If so, which encryption protocols should be utilized/meet the requirements of FIPS 140-2   Should additional NAESB Standards be evaluated to identify any unencrypted data communications and then modified to recommend an encryption method for those data communications   * If so, which encryption protocols should be utilized/meet the requirements of FIPS 140-2   Are there encrypted data communications that should be evaluated to ensure the encryption meets FIPS 140-2 requirements   * If so, which data communications and if the current encryption method does not meet the FIPS 140-2 requirements, should the standards be modified to recommend a specific method   Does the information provided by Sandia include enough detail to identify standard modifications related to verifying and validating all external inputs within the WEQ OASIS Standards   * If so, what standard changes should be considered   Should the WEQ OASIS Standards be modified to require annual business continuity and disaster recovery exercises  Should the WEQ OASIS Standards be modified to require applying patches/updates in a timely manner  Are there additional areas of the NAESB Standards that should be modified to require applying patches/updates in a timely manner |  | Dependent on identification of impacted standard areas |
|  | Business Operations Practices and Standards Report Section 6.1.1 – NAESB Standards Refer to Vulnerable Versions of Communication Protocols  NAESB standards contain references to specific versions of communication protocols that may be vulnerable to attacks discovered since the publication of those standards. For example, the standards require the use of the Secure Sockets Layer (SSL) protocol, which has been replaced by the Internet Engineering Task Force (IETF) with the Transport Layer Security (TLS) protocol  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 | For various reasons, including the potential of NAESB Standards to be acted upon by the FERC through the incorporation by reference process as well as compatibility and security considerations, it is not necessarily practical for the NAESB Standards to reference the latest version of a technology or protocol in lieu of a specific version.  Given this, should the following be considered by the subcommittees:  Evaluate the relevant standards (Business Operations Practices and Standards Report Appendix B) and make modifications to eliminate the use of the SSL protocol   * Evaluate the relevant standards (Business Operations Practices and Standards Report Appendix B) and make modifications to identify/update the minimum version of the TLS protocol and/or a timeline for which entities should update the version of TLS protocol following a new publication. * Evaluate the standards to identify any additional communication protocols (e.g. Hypertext Transfer Protocol, etc.) and as necessary identify/update the minimum version of the protocol and/or a timeline for which entities should update the version of the protocol following a new publication. |  | Dependent on identification of impacted standard areas |
|  | 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 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 10% the functionality could be flagged as deprecated and removed from the standard at the following annual review. The assessment team also recommends including a mechanism where an organization can request that the deprecated functionality be retained in the standards. | Should the subcommittees evaluate the standards and/or applicable specification to identify technical functionalities or requirements (e.g. security keys, Simple Object Access Protocol (SOAP) requirements, internet tool/accessibility requirements, etc.) and make modifications where necessary to update the technical functionality or requirement and/or remove legacy functionalities or requirements  Should this be a recurring annual plan item for the subcommittees |  | Dependent on identification of impacted standard areas |
|  | Business Operations Practices and Standards Report Section 6.2.1 – Use of Human Control and Review in Operations  Currently, business and control operations are performed or authorized by an individual who is familiar with normal operations…  With the current trend towards more automation and computer control, this strength should be considered when replacing human operators with autonomous systems. The assessment team recommends that, at a minimum, humans retain the ability to disengage any automated system and take manual control in the event of abnormal behavior or failure condition. In addition, operators should evaluate existing metering and sensors (pressure sensors, flow sensors, etc.) on a quarterly basis (or even daily for highly critical systems, if practical) to ensure that the automated/digital systems are reporting accurate information. | Does the information included by Sandia provide enough detail to define standard development activities to incorporate the use of human controls for specific areas of business and control operations  Should the subcommittees consider the need for standards to require the evaluation of the accuracy of automated/digital systems   * + If so, which subcommittees should perform this evaluation and what areas of the standards should be considered |  | Dependent on identification of impacted standard areas |
|  | Business Operations and Standards Report Section 6.2.2 – Separation of Business and Control Computer Networks  The EDI cyber attack that occurred in April 2018 illustrated the importance of maintaining separation of business and control networks. While the cyber attack against the EDI platform interrupted business functions, COOP procedures were utilized, and it was possible for the affected organizations to continue operations. If the control networks and business networks were connected, it is possible that the cyber attack would have prevented pipeline operations. | Does the information included by Sandia provide enough detail to define standard development activities regarding the separation of business and control networks |  | Dependent on identification of impacted standard areas |
|  | Business Operations and Standards Report Section 6.2.3 – Continued Use of Different Security Paradigms  Despite the increased connectivity between the gas and electric markets, both markets have continued to use their original security paradigms – PGP-based or PKI-based encryption…  The assessment team feels that, since both approaches provide for secure communications, each market should continue using their mature systems instead of all markets switching to a common technology… A switch to a different technology could result in vulnerabilities as system owners and administrators work to gain experience with and deploy the new systems.  However, the assessment team strongly encourages an organization to review the various threat models that have been defined by government agencies, industry groups, academia, and other organizations to determine what model will provide the most utility to their organization. | Are there additional factors not identified as considerations by Sandia that may require the evaluation of updating/upgrading cybersecurity communication protocols required by the standards |  | Dependent on identification of impacted standard areas |
|  | Addendum Report Section 2.2.1 – Adversary Models  There are a variety of adversary models that can be used to evaluate the capabilities of an adversary, each with their own strengths and weaknesses…  [Threat models] can be used to characterize different levels of adversaries and their related capabilities; and makes it easier to reevaluate adversaries based on their changing capabilities  [T]he assessment team strongly encourages an organization to review the various threat models that have been defined by government agencies, industry groups, academia, and other organizations to determine what model will provide the most utility to their organization | Does the information included by Sandia provide enough detail to define specific standard modifications beyond a recommendation for entities to consider the adoption of a threat model as part of cybersecurity plans |  | Dependent on identification of impacted standard areas |
|  | Addendum Report Section 2.2.2 – Attack Scenarios Against Current Operations  *An ACA issuing a certificate to a fictitious organization*: In this scenario, an attacker manages to convince an ACA to issue a certificate to a fictitious organization. It was indicated in the on-site meeting that, for someone to use this certificate to access OASIS, they would also need to be established in the EIR – which would require the attacker to have a level of presence suitable to make it through the various checks. (For example, it would actually have to be registered as a valid business with an appropriate Secretary of State or other official entity.) In addition, the organizational and individual authentication requirements for an ACA to issue a certificate are robust, and should prevent this from occurring. | Does the information included by Sandia provide enough detail regarding mitigation to identify specific standard modifications |  | Dependent on identification of impacted standard areas |
|  | Addendum Report Section 2.2.2 – Attack Scenarios Against Current Operations  *A pipeline could be stressed by over supply or over purchase of gas*: In this scenario, an organization (or an attacker able to impersonate the organization) nominates capacity or makes purchases that are outside appropriate bounds. In this scenario, it was indicated that the pipelines themselves would still deliver gas, but that there could be a commercial impact for upwards of three days. This scenario was mitigated since there are personal levels of involvement for each transaction. Specifically, that there is an individual who is managing the day-to-day transactions for each account, and that there is some level of personal relationship between organizations. Therefore, it was expected that large increases or decreases in nominated capacity would be noticed quickly, allowing human intervention before damage occurs. | Does the information included by Sandia provide enough detail regarding mitigation to identify specific standard modifications |  | Dependent on identification of impacted standard areas |
|  | Addendum Report Section 2.2.2. – Attack Scenarios Against Current Operations  *Nomination of, but failure to use, large quantity of capacity (and variations)*: From the discussion, it was expected that this scenario would be noticed within hours by the pipeline; or be noticed almost immediately by a shipper who had nominated capacity but had nothing flow. In addition, it was noted that the upstream and downstream confirmation process, and the other business processes in the background – such as billing – would make it difficult to manipulate the scheduled nomination for only a segment of the pipeline. It was also noted that, for wholesale gas, gas can only be delivered to the locations identified in the contract and cannot be diverted or redirected. In addition, excess/unused capacity can be easily sold on the spot market. | Does the information included by Sandia provide enough detail regarding mitigation to identify specific standard modifications |  | Dependent on identification of impacted standard areas |
|  | Addendum Report Section 2.2.2 – Attack Scenarios Against Current Operations  *Malicious modification of nominations*: This scenario can involve the modification of a nomination or a denial of service against the submission of a nomination. From the on-site discussion, it was determined that there are several business processes involved in nominating, scheduling, and billing that occur in each nomination period. In addition, it was indicated that these generally use different software packages and are monitored by a variety of individuals at an organization – essentially putting a human in the loop (or multiple humans) when it comes to the flow of gas. In addition, it was noted that the relationships between organizations are generally assigned to specific individuals, resulting in the individual being aware of normal business needs and requirements. | Does the information included by Sandia provide enough detail regarding mitigation to identify specific standard modifications |  | Dependent on identification of impacted standard areas |
|  | Addendum Report Section 2.2.2 – Attack Scenarios Against Current Operations  *An attacker able to steal an organization’s certificate/credentials for OASIS*: In this scenario, an attacker can obtain access to OASIS by impersonating an organization with legitimate access. During the discussion, it was noted that, since any action taken on OASIS is viewable by all parties, the organization that had their credentials stolen would be able to see any malicious activity done by the attacker impersonating them and be able to take remediation measures. (Such as communicating a compromise of their certificate to the ACA, trading partners, etc. and utilizing alternate channels to conduct business.) | Does the information included by Sandia provide enough detail regarding mitigation to identify specific standard modifications |  | Dependent on identification of impacted standard areas |
|  | Addendum Report Section 2.2.2 – Attack Scenarios Against Current Operations  *Compromise of an ACA*: In this scenario, a capable adversary – such as a nation-state – is able to compromise the certificate authority, bringing into question any certificates that they have issued. This scenario is of concern to the ACA themselves, and they take active measures to prevent this scenario. It was also noted that, in general, organizations have alternative contact information (phone, fax, etc.) for their partners, which would allow them to set up alternative mechanisms for conducting business. | Does the information included by Sandia provide enough detail regarding mitigation to identify specific standard modifications |  | Dependent on identification of impacted standard areas |
|  | Addendum Report Section 2.2.2 – Attack Scenarios Against Current Operations  *Backend system security*: It was noted in the on-site meeting that the industry has purposefully chosen to not address this through the NAESB standards. | Does the information included by Sandia provide enough detail regarding mitigation to identify specific standard modifications |  | Dependent on identification of impacted standard areas |
|  | Addendum Report Section 2.3.1 – EDI Cyber Attack  To better understand the impact this kind of outage has on business operations and operating costs, the team has identified several metrics that could be used to help quantify the impact of these kinds of events:   * Measure the number of daily transactions during normal operations and the number of daily transactions when using COOP procedures. * Measure the number of hours worked by staff during normal operations and during COOP procedures. This should also include any time spent on recovering local systems or testing to ensure functionality of remote systems has been restored. * Measure any additional expenses incurred due to utilizing COOP procedures. For example, if food must be provided due to staff working additional hours; or expenses due to overtime wages. * Measure the number of errors made in transactions during normal operations, and the number of errors made when using COOP procedures. * Measure the time the outage began, to the time full service is restored. * Measure the time and expense to perform a forensic analysis of affected systems to determine the root cause of the attack or failure.   Count the number of organizations affected by the outage.  Following a major outage, these metrics could be reported to NAESB to tabulate the total cost and impact of the event. This data could then be used in life-cycle decisions, vendor selection, analysis of continuity of operations/disaster recovery planning, and to determine if NAESB standards need to be upgraded or revised. | Is it appropriate for any potential metrics to be reported to NAESB as the organization is not involved in any aspect of compliance or compliance management  Should each quadrant consider the development of standards to identify the reporting process following a cyber attack and/or the minimum information entities should make available   * + Does the information provided by Sandia provide enough detail or resources to identify the basis for such standards development activity |  | Dependent on identification of impacted standard areas |
|  | Addendum Report Section 2.3.2 – Ukrainian Power Grid Attack  A true air-gap between the business and control networks would have prevented the attacker from pivoting into the SCADA network and gaining control of the Human-machine Interface (HMI) systems that allowed them to control the breakers. If an organization requires a connected between these networks (or the SCADA network and the Internet) to exist – even for a brief period of time (ex. to download firmware updates) the connection should be restricted to only authorized traffic and individuals, it should use robust authentication methods such as two-factor authentication, whitelisting of IP addresses, and monitoring to ensure that only authorized operations are performed while the connection exists.  ICS-CERT issued an alert, “Cyber-Attack Against Ukrainian Critical Infrastructure” ([IR-ALERT-H-16-056-01](https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01)) regarding the incident, and this report provides a brief description of the event, and recommended mitigations. These mitigations discuss applying best practices across the entire business and operations space, which include: supply chain risk management, asset tracking, user tracking, system maintenance and updates, and “strategic technology refresh”. Of note is that they recommended contingency plans for continuity of operations and system shutdown. The full list of recommended mitigations and links to other resources, can be found in the ICS-CERT report. ICS-CERT also maintains a “[Recommended Practices](https://ics-cert.us-cert.gov/Recommended-Practices)” site that provides additional guidance on securing OT networks, including any connections to IT networks. | Are there areas within the standards that currently use single-factor authentication (e.g. website logins, email protocols, electronic communications, etc.) which should be updated to require the use of two-factor authentication (such as PKI or other methods)  Should the standards require entities to create, maintain, and make available (where applicable) a trusted list of IP addresses or IP ranges from which users can access domains (IP whitelisting) or specific sites (e.g. OASIS nodes, EBBs/Internet Electronic Transport sites)  Should the NAESB standards address access monitoring for specific applications (e.g. OASIS nodes, EBBs/Internet Electronic Transfer sites, etc.)  Are there additional recommendations from the IR-ALERT-H-16-056-01 or ICS-CERT Recommended Practices that should be addressed within the standards |  | Dependent on identification of impacted standard areas |
|  | Addendum Report Section 3.1 – Trends in Operations  As technology is integrated into the control systems, it is important to ensure that abnormal events can be detected and that abnormal conditions do not prevent operations from being conducted or, after an outage, from being restored.  To ensure that problems can be detected, the assessment team recommends that existing metering be used to verify information being provided by the control systems and, in the event that the computer system and the metering system disagree, that response personnel can be deployed to investigate in a timely manner. However, to ensure that response personnel are able to manually restore proper functioning, the assessment team notes it is imperative that the responders have a method to disconnect the equipment from the control network and conduct manual operations until normal operations can be restored. | Are there areas already included in the standards or that should be added to the standards to address manual verification of automated metering  Should the standards address circumstances necessitating a need to switch from automated to manual operations of equipment   * + If so, which systems/operations/equipment should be addressed and should the standards also address requirements for these manual operation periods or reintroducing automation |  | Dependent on identification of impacted standard areas |
|  | Addendum Report – Section 3.1 Trends  [A]s new technologies such as cloud computing, mobile device integration, and real-time communications are adopted, these create new cyber security challenges and could provide an adversary with an attack vector against utility companies.  To address the security of the various technologies listed above, the assessment team recommends that organizations utilize the government and industry standards that are relevant to the technologies deployed…  [NIST SP 500-299](http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Reference_Architecture_2013.05.15_v1.0.pdf): NIST Cloud Computing Security Reference Architecture (Draft)  [NIST SP 800-144](http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf): Guidelines on Security and Privacy in Public Cloud Computing, December 2011  [NIST SP 800-145](http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf): NIST Definition of Cloud Computing, September 2011  [NIST SP 800-146](http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf): Cloud Computing Synopsis and Recommendations, May 2012  NIST also maintains a [page](https://www.nist.gov/topics/internet-things-iot) related to the Internet of Things (IoT) that includes reports related to trust, fog computing (cloud computing for IoT), and other areas related to the IoT.  Other resources provided by NIST that address the above technology include:  [NIST 800-124rev1](https://csrc.nist.gov/publications/detail/sp/800-124/rev-1/final): Guidelines for Managing the Security of Mobile Devices in the Enterprise  [NISTIR 8144 (DRAFT)](https://www.nccoe.nist.gov/sites/default/files/library/mtc-nistir-8144-draft.pdf): Assessing Threats to Mobile Devices and Infrastructure - The Mobile Threat Catalog  [NCCoE Project](https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/cloud-hybrid): Mobile Device Security: Cloud and Hybrid Builds | Should the NAESB standards identify the NIST guidelines as recommended standards entities should follow to address new technologies such as cloud computing, mobile device integration, real-time communications, and the IoT  Are there specific recommendations within the NIST reference documents identified by Sandia that the quadrants should consider for incorporation into the standards to address cloud computing, mobile device integration, real-time communications, and the IoT. |  | Dependent on identification of impacted standard areas |
|  | Addendum Report Section 3.1 – Trends in Operations  [A]s new technologies such as cloud computing, mobile device integration, and real-time communications are adopted, these create new cyber security challenges and could provide an adversary with an attack vector against utility companies.  The assessment team recommends that, prior to the adoption and deployment of new technologies, organizations investigate what it takes to operate the systems in secure manner by reviewing resources provided by NIST, ICS-CERT, and other government organizations. (For example, DHS maintains a portal for their [cybersecurity resources](https://www.dhs.gov/science-and-technology/csd-resources).) This will ensure that operations can be properly secured prior to deployment of the new systems and technologies, ensuring new attack vectors are not introduced. | Should the standards identify potential resources for entities to consider prior to the deployment of new technologies |  | Dependent on identification of impacted standard areas |
|  | Addendum Report Section 3.2 – Recommended Future Assessments  Since OASIS nodes are implemented independently, the team recommends conducting scans or penetration tests of the various nodes to identify any nodes that are using older software versions, leak information about the system (ex. list software versions being used), or have vulnerable implementations of their web applications. Since each node could be unique in its software, environment, and supporting security systems, the assessment team recommends that the node owner perform these assessments on their own systems. | Should the WEQ OASIS Standards be modified to recommend OASIS node owners conduct software, environment, and supporting security system assessments |  | WEQ OASIS Subcommittee |
|  | Addendum Report Section 3.2 – Recommended Future Assessments  Perform security assessments on software, services or platforms (SPPs) that are used by more than 10% of organizations or carry more than 10% of total transactions as measured by volume or dollar value. This percentage can be adjusted based on operational needs and total number of SSPs that fall within this range. In addition, the assessment team recommends that this be performed on an annual basis, or anytime there is a major update to a specific SSP. The assessment team recommends that software vendors, in partnership with their customers, determine specifics of these assessments to ensure that all relevant risks are addressed. | Should the applicable WEQ/WGQ/RMQ standards be modified to recommend entities require software vendors perform an assessment on utilized systems to ensure all relevant risks are being addressed   * + If so, which software/applications should be included (e.g. e-Tagging systems, pipeline systems, WGQ/RMQ Internet Electronic Transport-based software, etc.)   + If so, should a frequency of the assessment be specified |  | Dependent on identification of impacted standard areas |