Dear NAESB,

Per your request, below find SSL.com’s comments in relation to the draft reports provided by Sandia National Laboratories on January 25, 2019.

We are specifically commenting on the three recommendations impacting WEQ-012/Accreditation Requirements for ACAs:

1. PKI Report – Section 6.1.1 Discrepancy between NAESB Standards and Certification Practice Statements

**Sandia Finding:** Language differences between the NAESB standards and CPS allow for a window of time where the CPS does not match the NAESB requirements and could result in non-compliant certificate operations

**Sandia Analysis:** The GlobalSign and OATI CPS’s include NAESB specific language that is drawn from various NAESB standards. For example, the GlobalSign CPS includes text regarding the NAESB Authentication Requirements; and the OATI CPS includes text regarding cases where a certificate can be revoked. However, Section 1.5.4 *CPS Approval Procedures* of the GlobalSign CPS indicates the CPS will be updated on an “as needed” basis; and Section 2.3 *Certification Practice Statement Management* of the OATI CPS indicates it will be reviewed “at least annually and updated as necessary to reflect changes to applicable industry standards.”

**Sandia Recommendation:** 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.

**SSL.com Comments:** There is sufficient information to move forward with this requirement. Changes are needed to the WEQ-012/Accreditation Requirements for ACAs to mandate that any CPS must clearly indicate audits are done against the “current versions” of the WEQ-012/Accreditation Requirements for ACAs. For example, SSL.com’s CPS includes the text:

The SSL.com CP/CPS also observes the most current versions of the following:

OATI’s CPS section “10.1 External Audits” similarly states:

The practices in this CPS are designed to meet or exceed the requirements of generally accepted industry standards, including the latest versions of NAESB WEQ-012, and the AICPA/CICA WebTrust Program for Certification Authorities (WebTrust). This CPS also conforms to the current version of the CA/B Forum BRs published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

1. PKI Report – Section 6.1.2 Possible Incomplete Enforcement of NAESB Standards Assurance Levels

**Sandia Finding:** CPS stated audit log retention periods do not enforce full coverage of all assurance levels as dictated by the NAESB standards.

**Sandia Analysis:** The GlobalSign CPS indicates that they retain audit logs for a period of “at least 10 years” (Section 5.4.3 *Retention Period for Audit Log*). This length of time meets the NAESB requirements for “Rudimentary”, “Basic”, and “Medium” assurance levels found in Section 4.5.2 of the *NAESB Accreditation Requirements for Authorized Certification Authorities*; however, the retention period for the “High” assurance level is given as 20 years. Since NAESB tools only requires a certificate at the “Basic” assurance level, it is unclear if “High” assurance level certificates have been issued.

**Sandia Recommendation:** 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”.)

**SSL.com Comments:** There is sufficient information to move forward with this requirement. SSL.com believes no ACA is currently issuing certificates at a level other than Basic Assurance level. However, changes are needed to the WEQ-012/Accreditation Requirements for ACAs so that an ACA’s CPS must clearly indicate 1) at what assurance level the ACA has issued certificates and 2) that records shall be retained for “time periods required by the applicable standards and assurance level”.

1. PKI Report – Section 6.3 Review of X.509 Security

**Sandia Recommendation:** 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.

**SSL.com Comments:** There is sufficient information to move forward with this recommendation. SSL.com believes organizations that rely on X.509 certificates (“Relying Parties”) must carefully monitor details on individual CVEs and update their systems and software to quickly eliminate any risks or vulnerabilities. Implementation of this recommendation can be explored by the NAESB Cyber Security Subcommittee but enforcement would most likely need to come from somewhere other than the WEQ-012/Accreditation Requirements for ACAs.

We appreciate this opportunity to communicate our observations and welcome any questions or thoughts you have regarding these comments.

Regards,

Chris Kemmerer

Compliance Manager
SSL.com

February 5 2019