RESPONSE TO REQUEST FOR PUBLIC COMMENT
NAESB Retail Energy Quadrant (RXQ) Request for Formal Comments on 2014 Retail Annual Plan Item 6.b Recommendation

NAESB Specification for Data Privacy Governing Third Party Access

RESPONSE FILED BY:
Rebecca Herold & Associates, LLC

We submit the following comments on behalf of Rebecca Herold & Associates, LLC dba The Privacy Professor®.

Summary of draft document intent:

The draft NAESB document "provides the technical and managerial details that a Third Party must demonstrate that it meets in its Certification Practice Statement. The following requirements are intended to support the NAESB REQ Model Business Practice Standards for Third Party Access to Smart Meter-based Information."

About Rebecca Herold & Associates, LLC

Rebecca Herold & Associates, LLC, dba The Privacy Professor® (Rebecca), has over 25 years of privacy and information security experience. Rebecca has performed over 250 third party privacy and information security compliance program audit/reviews. Rebecca has led the NIST SGIP SGCC Privacy Group since 2009 when it was formed, and has experience in performing certification reviews for PCI-DSS, US-EU Safe Harbor, and ISO 27001 ISMS. Rebecca also just completed researching and co-authoring a book on smart grid privacy[1]. See more about Rebecca at www.privacyguidance.com.

General Comments

We welcome the opportunity to review the components involved with the proposal to establish a certification process for third parties that have been entrusted by utilities, and possibly consumers, with access to personal information and consumer energy usage data (CEUD). Requiring third parties validation of their safeguards is of growing importance as we see that efforts to ensure third party safeguards are in place are getting worse[2] while the

---

[1] The book is "Data Privacy for the Smart Grid" will be published in January 2015 by CRC Press. See more at http://www.crcpress.com/product/isbn/9781466573376.

[2] Per CSO Online, "fewer organizations -- 44 percent this year compared to 54 percent last year -- are bothering to put in the effort to vet the security of third party providers and others in their IT supply chain." Published July 28, 2014 at http://www.csoonline.com/article/2458048/security-leadership/insecure-connections-enterprises-hacked-after-neglecting-third-party-risks.html

625 42nd Street
Des Moines, Iowa 50312
http://www.privacyguidance.com
515-491-1564 *tel*

numbers of privacy breaches caused by third parties are rising significantly[3].

Validations in the form of a certification of some sort has long been a method used to determine appropriate due diligence. An important point about certifications is that the complexities of validating the operational/administrative, physical and technical components of an organization's privacy and information security program components, and the associated actions, are many and must be appropriately implemented so that

1) those seeing the privacy program certification do not interpret it to be a certification of outcome; they should not interpret the certification to indicate that privacy is guaranteed (as technical certifications often guarantee hardware or software components meet minimum specifications and, as such, will not change as business activities occur), and
2) that the certification requirements are comprehensive and do not omit important components that will leave the entity, along with their customers, with a false sense of assurance with regard to the privacy, as well as security of their information.

We appreciate the attention to privacy assurance that NAESB is making as demonstrated by this privacy certification initiative. We fully support efforts to help ensure any and all entities are protecting privacy appropriately and in a feasible manner. However, we offer in this paper our concerns about the proposal, in its current form, and offer recommendations for improvement. We understand that NAESB be reviewing these submissions, and we appreciate the opportunity to present additional comments.

A. Comments to specific sections within the Draft NAESB Specification for Data Privacy Governing Third Party Access

1. **Section 2.6: Definition of "Third Party**." Clarify whether this is always an entity that has direct relationship with a utility, or if this can also be an entity that communicates with the utility Retail Customer and that has no obligation and/or communication with a utility.
2. **Section 3.6: Security and Safeguard Practices Requirements**. This section is vague and open to interpretation to the certification assessor. For any effective privacy and information security certification, the details of all the necessary actions, documentation and components are of utmost importance. Without them you will have similar entities possessing the same certification that have dramatically different safeguards established. Details are important. Include the details for all the safeguards that an entity must have in place to be certified. Without such details a certification is weak and ineffective.
3. **Section 3: Certification Practice Statement.** What is the acceptable format for a

[3] According to the Identity Theft Resource Center's 2013 Breach Report, breaches from third parties accounted for 14.3% of total privacy breaches in 2013, reflecting a 66% increase over third party-caused breaches in 2012. This represents 614 known breaches, exposing the records of 91,982,172 individuals. Accessed from http://www.idtheftcenter.org/images/breach/2013/SubcontractorSummary2013.pdf on July 28, 2014.

625 42nd Street
Des Moines, Iowa 50312
http://www.privacyguidance.com
515-491-1564 tel

"Certification Practice Statement"? Is there a template that will be provided for this purpose? Will this be a digital seal that can be verified by a click through from it to the official certification statement? This statement will need to be clearly detailed, and use of it controlled and monitored.

4. **Section 3.6.2: Privacy Use Cases.** NISTIR 7628 Volume 2 Revision 1 contains 44 examples of smart grid privacy use cases. We recommend you point to that for the readers to see full examples of use cases, in addition to pointing to REQ.22.3.8.2.1.3.

B. General Comments, Considerations and Recommendations

1. **Who performs the certification?** The wording provided implies, but does not state explicitly, that the third party is self-certifying. The acceptable ways in which certification may occur should be clearly described, and the question of who is appropriate to certify should be answered. There are three common ways in which an entity can certify they are complying with all requirements of a specified standard/contract/regulation/etc. These include the following, along with the indicated benefits and drawbacks:
    a. Self-certification[4].
        i. Benefits:
            1. The least expensive of the certification options to the third party undergoing certification.
            2. Establishes some accountability for the entity doing the self-certification.
        ii. Drawbacks:
            1. As history has demonstrated with other self-certification programs, many entities will self-certify without actually performing the required actions, making the certification untrustworthy.
            2. Without an oversight entity to audit the certifications and validate compliance, as well as sanction non-compliance, there will be a false sense of privacy from the public for all the entities that do not actually have the elements necessary to qualify for the certification.
    b. Independent third party certification.
        i. Benefits:
            1. Third party validation of controls and practices is objective, not biased, and more accurate than self-certification.
            2. The audits performed by a wide number of qualified certification agencies will be auditing against the same standard, making the results repeatable from one certification audit agency to another.
        ii. Drawbacks:

[4] To see the US-EU Safe Harbor self-certification process, as an example, see http://www.export.gov/safeharbor.

625 42nd Street
Des Moines, Iowa 50312
http://www.privacyguidance.com
515-491-1564 tel

1. Independent certification audits will be more expensive than self-certification.
2. The third party doing the certification may not be well-qualified to perform the certification audit. As seen in other industries, when new revenue opportunities appear, a significant portion of individuals and businesses will take advantage and offer services (certification audits) for which they are not qualified.

c. Certification from an accredited body.
   i. Benefits:
      1. The 3rd party certification auditor is vetted by some type of oversight committee and determined to know what they are doing.
   ii. Drawbacks:
      1. The most expensive of all certifications.
      2. There must be a process created (by NAESB or some other non-profit oversight) to accredit the certification auditor.
      3. The oversight agency may be accused of playing favorites in accrediting the audit entities.

d. Recommendation.
   i. We recommend there be two levels of certification:
      1. Self-certification with a seal or certification report or label clearly indicating the certification was performed internally.
      2. Independent third party certification, with a different seal or certification report or label clearly indicating the certification was performed by an independent third party that is clearly named.
   ii. Benefits:
      1. This will allow for entities with different budgets to participate in the certification programs.
      2. This will allow those seeing the certifications to quickly know the level of independence and reliance that can be placed in the certification; the objective certification will carry more weight and trust than the self-certification, but the self-certification will still show that the entity is establishing accountability and liability by self-certifying.

2. **Is this a certification for guaranteeing an outcome (privacy), or for validating the existence of privacy program elements?** The connotation in most of the clients I've spoken with about security and/or privacy certification is that they view it as a guarantee that privacy and/or security is guaranteed if an entity is certified. However, as the growing number of criticisms for PCI DSS certification demonstrate, it is clear that the description of what is being certified must be clearly described, and expectations must be set to point out that even with the most rigorous due diligence, privacy breaches may occur for a wide variety of reasons.
3. **Include training and awareness as a certification requirement**. There is not requirement for those with access to Smart Meter-based Information to take regular privacy training and receive ongoing awareness communications to help them

625 42nd Street
Des Moines, Iowa 50312
http://www.privacyguidance.com
515-491-1564 tel

understand how to appropriate protect the privacy of the information that they are working with as part of their daily job activities.

4. **Clearly detail the acceptable forms of demonstrating compliance.** To have a consistently applied certification there must be a common base set of documentation standards that all certified bodies should be required to meet. If these are not well-defined, each entity will interpret what it means to "demonstrate" each compliance activity, and significant vulnerabilities and threats could exist within a certified entity as a result.
5. **Require some type of assurance for subcontracted entities.** If the third party subcontracts activities, there should be demonstrated, documented (in a consistent manner for all certified entities) that reasonable assurances are made to ensure the subcontracted entity is appropriately addressing privacy.
6. **Include requirements for disposal.** Many significant privacy breaches have occurred as a result of improper and unsecure disposal of information, in all forms, and on all types of storage devices, computers and hard copy media. Include certification requirements for the proper and irreversible disposal of information in all forms.
7. **Include all the REQ.22.3.8.2.1.3 requirements**. Providing only a subset of the full set of privacy program requirements will result in leaving vulnerabilities and threats that are not addressed. A certification must necessarily be rigorous and comprehensive, as well as repeatable. If a certification is not rigorous and comprehensive, then it fails to serve the purpose for which is was created; to accurately as possible indicate that a privacy program is fully addressing all privacy risks within the entity's privacy program and supported activities.

625 42nd Street
Des Moines, Iowa 50312
http://www.privacyguidance.com
515-491-1564 *tel*