20120110 Minutes

1. Open Items
   a. Updating the AMI use cases in the NISTIR 7628.
      i. We need to use the format currently in the NISTIR 7628 chapter 10 for any updates.
      ii. Sandy will take our eight use cases and format them in the current NISTIR 7628 chapter 10 format.
      iii. After the writing is complete, we will review for any updates to all of the NISTIR 7628 AMI use cases. Our review can be for more specifics in the content or less, we will use our team consensus.
   b. We have had a few questions on how to use the AMI Security Profile. The ASAP-SG developed a document on "How a Utility Can Use ASAP-SG Security Profiles": [http://www.smartgridipedia.org/images/1/1b/Using_security_profiles_v0-12_20111020.pdf](http://www.smartgridipedia.org/images/1/1b/Using_security_profiles_v0-12_20111020.pdf).
      i. There was a mixing of "shall" and "must". Sandy updated all the requirements to ensure we are consistent with "shall" and the changes are bolded and in purple font color. Sandy will ensure that our profile document has the IEEE or RFC definition for shall.
      ii. Sandy struck out the word "strong" throughout all the requirements and it did not appear to change the requirement.
      iii. Sandy validated the consistent use of "secure" and "securely" within the requirements and the changes are bolded in purple font. Sandy will ensure that our profile document has a basic definition of "secure" and "securely".
      iv. Sandy validated the use of "such as" (e.g. row 32 and row 73) in the requirements. When we use the term "such as" we are specifying examples. It was suggested that we use a comma (,) preceding "such as". Sandy will validate for consistency.
      v. Rather than reinventing requirements, if there is a source that contains good language for authentication, certificates, cryptography, then we should use it.
      vi. Identification & Authorization.03 (Digital Certificates), Identification & Authorization.04 (Two Factor Authentication), and Identification & Authorization.05 (Device Identification and Authentication) has a large discussion.
         1. We know that identification and authentication are requirements.
         2. We also know that some of the technology today cannot support what is really needed for identification and authentication. The requirements need to be written for what we need for identification and authentication.
         3. We need to distinguish between human and device interactions for identification and authentication.
         4. Sandy will craft new requirements specifically for human authentication and device authentication and complimentary identification requirements for review next week. Some redundancy in the new requirements is good.
      vii. System & Communication Protection.10 (Communication Integrity). Change phase “an approved published protocol” to “an approved published protocol or standard” with a footnote of “Examples of a few organizations that publish protocols or standards are IEEE, IEC, ISO, ISA, ANSI, W3C, CSA, ITU, and IETF".
2. Open floor.
   a. None.
3. Attendees
   a. Alan Rivaldo
   b. Amanda Stallings
   c. Avygdor Moise
   d. Barbara Fraser
   e. Doug McGinnis
   f. Irene Gassko
   g. Jeffrey Sweet
   h. Kevin Lackey
   i. Richard Bockenek
   j. Sandy Bacik
   k. Shrinath Eswarahally

Regards,
Sandy Bacik, CISSP, CISM, ISSMP, CGEIT
Principal Consultant
EnerNeX
p: 865.696.4470
e: sandy.bacik@enernex.com // www.enernex.com