**Annie’s Notes on the NAESB Work Paper – Sandia Surety Assessment**

3. Reviewing the database for applicable threats is great idea, but would require some level of effort. Given that NAESB is also involved in the response to broader threats to the industry, perhaps review of the database is part of a broader “state of cyber issues” that NAESB reviews each year, such as incidents, that might precipitate change to a standard.

5. Mentioned in #10 below, encryption is probably a topic for a standalone meeting. FIPS is a good place to start, but other questions include the asset owners’ ability to change or update, vendor technology roadmaps, etc. With regard to patching/updating, most asset owners in the operational space develop their patching/change management procedures based on criticality of both the vulnerability to be patched, and the system to be patched. Asset owners are also subject to the approval of the patch by their vendors (making sure a patch won’t break the software). An example would be “critical patches are applied within 3 days of vendor approval”, and so on. This is dependent on the asset owner’s ability to apply those patches. To avoid the details, NAESB could make a recommendation that asset owners identify procedures within their own policies to ensure critical patches and security updates are applied as soon as possible, and commensurate with risks to operations.

6. The first paragraph in the Considerations column is spot on. Listing exact versions of software is difficult in a standard. That said, TLS v 1.0, for example is riddled with vulnerabilities and not even used in much of the new mobile technologies, etc. One option is for NAESB to recommend *not* using vulnerable versions (like TLS 1.0), and instead using the latest versions. They may also make a recommendation that an asset owner upgrade within a certain period of time when a version is identified as vulnerable.

7. Reviewing and updating the technical measures listed in the standard is a great idea, and ambitious. Many other standards organizations have tried this on an annual basis and it almost always takes longer. Then again, NAESB committees are very productive!!

8. Human verification is always helpful, but technology exists to monitor equipment and alert asset owners if a device begins to operate outside normal parameters, or the health of the system fails. This monitoring technology is already well ingrained into operational environments. Other research projects have drafted best practices for implementing this technology, and standards exist in some sub-sectors regarding alerting. You could simply point to the work already done.

9. Separation of IT/OT environments is addressed in nearly all standards, and most vendors subscribe to the PERA (Purdue Enterprise Reference Architecture) as a model. This relates to #20 below.

10. Definitely need to address, at a more technical level, any encryption recommendations. In 2006, this area caused significant discussion among our evaluation team. Addressing encryption in standards can be tricky, you do not want to impede operations, but the data must remain secure. I think this area is probably a standalone conversation just about NAESB’s position on sufficient encryption models and implementation.

11. Adversary models are interesting and it can be useful to understand the possible threats but I don’t think this information provides detailed technical metrics that would be addressed in the standards.

12-18: These areas probably need a deep dive discussion. The risks need to be addressed at the application and network level, including consideration of any data protections, both for data at risk and in transit.

19. This is a great idea…but ….the challenge here is handling the compliance information. I’m not sure the ramifications to a NAESB. This oil & gas industry have tried a dozen different ways to share info like this, and none have been successful. Handling this info, storing, divulging, and the potential impacts on share price, etc., seem complicated from a legal standpoint. NAESB lawyers will know best on this one!

20. Most of the operational best practices in the industry now make the recommendation to use two-factor, white-listing, etc., but include the caveat “in areas where operations and safety are not impacted”. You could do something similar hear but structure some parameters. You don’t want to give an operator the ability to ignore these controls. Instead, you want to encourage them to use these controls with careful configuration and implementation. There are many resources out there that can guide detailed configuration of white listing, authentication, etc.

The big point here, both with the Ukrainian attack and the EDI incident, is that air gap is not realistic. Instead, an owner needs to follow the recommended practices of separating the IT/OT environment through network security controls. There are countless models, detailed guides out there to do this. That separation has been an industry recommendation since the very beginning.

21. It will be interesting to see what the committee things on this one. Some vendors, like Emerson, state that their meter verification solutions serve as a measure of compliance for the big agencies, but it doesn’t seem like the vendors reference existing standards.

22. NIST standards are a good starting point and should be included as a recommendation. However, there are many other standards relevant to each subsector (and NAESB quadrant). Some of these have been drafted to complement federal guidelines. You could probably combine this with resources in #23.

23. This is always a good idea, but the resources and locations probably change faster than the standard, so you may want a caveat sentence “sources x,y,z plus any new and relevant resources from these entities” etc.

24. Yes, per #25 below, this would fall in line with other standards. In both the operational and IT environments, most owners find that they need to do some level of independent assessment, either because the vendor’s assessment does not exist or is not satisfactory, or they need to measure findings within their organization’s own risk portfolio.

25. NAESB could recommend that end users require vendors to have an independent assessment of the technology, this would echo other industry standards. (i.e. TSA pipeline security guidance shifted from recommending an assessment on critical systems every 3 years, to every year in the new 2018 guidance).