

MEMORANDUM

Attention: Sarah McKinley

Re: Introductory Comments – FERC Panel, Jan 31,2011

Before I begin, I would like to complement the NIST team for their excellent work developing NISTIR 7628. NISTIR's 197 requirements align well with other frameworks, such as those offered by the International Society for Automation (ISA) – known as ISA99 or IEC 62443.

In regards to content, the five core standards are a good start, but as currently written are neither comprehensive (communication centric) nor do they provide any specifications for security certification, which is required to build (and verify) security into Smart Grid products and services offered by system and component suppliers.

In regards to process, U.S. participants representing Owner/Operators was very limited. As a result, the initial development of the IEC standards cited is not comprehensive from an operational security point of view.

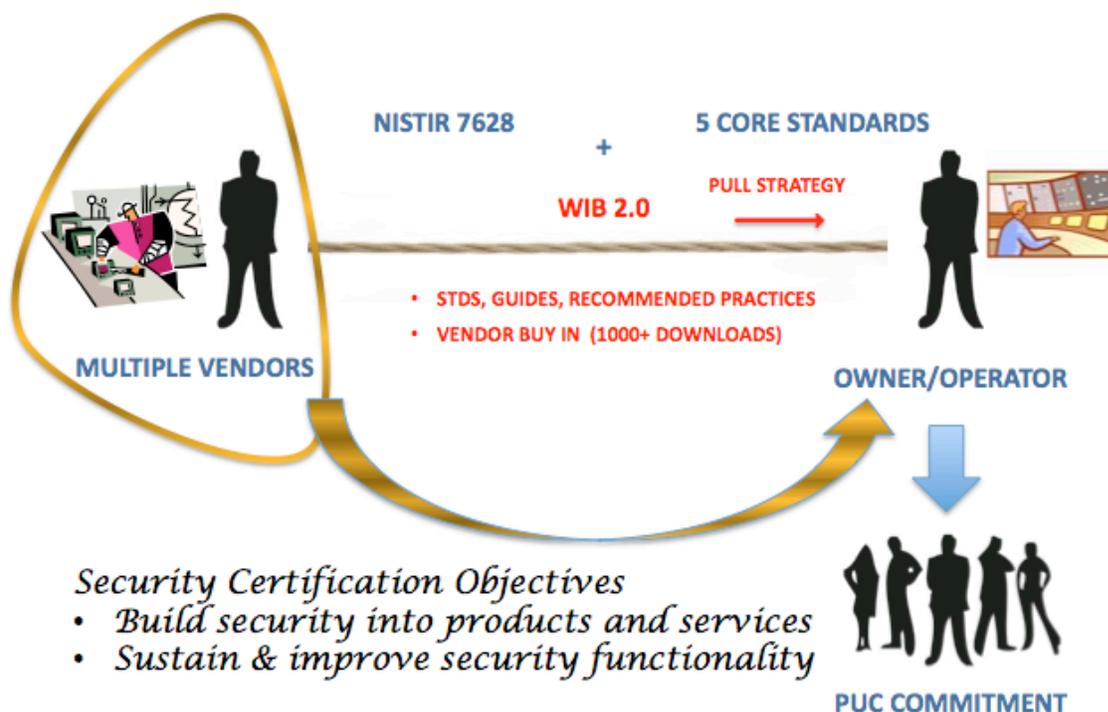
In contrast, consider the WIB 2.0 (October 2010) requirements, offered by The International Instrument Users' Association. WIB security requirements coupled with vetted Vendor evidence requirements for certification are in place and successfully tested for Smart Grid Advanced Metering Infrastructure (AMI) systems and services. WIB vetting involved the leading suppliers and stakeholders to establish a solid consensus of the requirements for certification as well as validation by performing certifications, which improved the processes. I believe this approach is stronger than the approach to use "selected experts" to identify the five families of core standards.

Furthermore, I am concerned that many important contributions to design security into the Smart Grid infrastructure are not addressed by these families of core standards, but are addressed in other guidelines and recommended practices; patching for example. These contributions may not use the same security framework as IEC 62351, but do provide adequate security for a wider class of deployed Smart Grid components and systems. Wurldtech discovered this defect when testing Smart Grid AMI systems and services for security certification. One possible solution may be to include these additional guidelines as normative references thereby integrating them into the standards under consideration.

WIB 2.0 also offers the distinct advantage of strong asset owner/operator buy-in (they were integral in its development). This "pull strategy" results from major electrical power utilities telling their suppliers that to continue selling their products and services, they must successfully certify their security policies and practices. By the utility telling their Public Utility Commission (PUC) that Smart Grid systems are secure, this strong security requirement represents a commitment to the PUC.

The approach offered by WIB (end user driven, certifiable, operational security requirements) has gained serious recognition and momentum across a wide-range of process control communities, including the energy sector. Since posting WIB 2.0 on their web site in November 2010, vendors providing products and services to the process control industry have requested over 1000 downloads. Many of these vendors provide products and services for the Smart Grid, which again proves the strength of support and consensus to adopt and implement the WIB requirements.

The figure below details my recommendations pictorially.



In conclusion, NIST has provided an excellent framework of Smart Grid security requirements in NISTIR 7628. The five core standards recommended are an excellent first start. Add WIB 2.0 to the mix: vet with the large utilities who must operate this equipment safely and securely, and you have fixed the glaring defects.

Yours truly,

Dr. Nate Kube, CTO