

Statement of Darren Reece Highfill

Founder, UtiliSec

Before the United States of America Federal Energy Regulatory Commission

Technical Conference on Smart Grid Interoperability Standards

January 31, 2011

Statement of Darren Reece Highfill
Founder, UtiliSec
January 31, 2011

Good afternoon, Chairman Wellinghoff, Commissioners, and staff of the Federal Energy Regulatory Commission. I would like to thank all of you for this opportunity to speak to the issue of smart grid standards recommended by the National Institute of Standards and Technology (NIST) for consideration in a rulemaking. My name is Darren Highfill, and while my personal clientele includes investor-owned utilities and the U.S. Department of Energy, I am here today as an independent consultant serving in several industry roles relevant to smart grid standards. Specifically, I am the Chair of the Smart Grid Security Working Group within the Utility Communications Architecture International Users Group (UCAIug), a member of International Electrotechnical Commission Technical Committee 57 Working Group 15 (IEC TC57 WG15 – the group responsible for IEC 62351), and an active participant and subgroup lead in the NIST Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG). Today I will speak to two primary issues: the process for achieving consensus on the five IEC standards recommended to FERC by NIST, and considerations for implementation of technical standards through regulation.

Since the passage of the Energy Independence and Security Act of 2007 (EISA 2007), NIST has spared no effort in its coordination of building an interoperability framework for the smart grid. The last three years have witnessed a monumental push by the entire industry to accelerate this work. NIST should be given credit for achieving some remarkable accomplishments while undertaking a broadly-defined task of enormous scope and complexity. Under NIST's leadership we have created a conceptual model with which to frame our industry, established a forum for all stakeholders to discuss and resolve issues, and instituted a central clearing house for publishing smart grid information. However our processes were not wholly and perfectly conceived at the outset, and thus have changed as we have learned. We must continue to learn as we move forward, and therefore would benefit from consideration of some specific items in the evolution of these processes.

While NIST has established a process that includes checks and balances, we must still consider and refine the weighting of the stakeholder representation model in light of the impact upon specific stakeholder groups as well as the overall industry. Currently the SGIP is structured such that someone who decides to open a one-person business has the same vote as a utility that is responsible for safely, reliably, and cost effectively serving millions of customers. This person may have no background or understanding of the industry and no investment in the process beyond registration with the SGIP, yet it is this very process that will most directly determine the future of our utility's systems. The entrepreneur plays an important role in this ecosystem, but we must also recognize the importance of wisdom, experience, responsibility, and accountability. Our process for achieving consensus needs to align with what is at stake for industry and society, and it will require our collective effort, focus, and time to get it right.

Unfortunately time is not an asset this industry has been offered. While placing a national priority on the smart grid sounded good to me as a technologist, it has also created a political environment with extreme pressures and forced leaders to weigh expedition against technical integrity. Make no mistake that the realities of strong political pressure take a toll on development, understanding, and execution of complicated technical processes – and the smart grid is nothing if not complicated. The process used

Statement of Darren Reece Highfill
Founder, UtiliSec
January 31, 2011

to achieve consensus on the five IEC standards was sincere, however it was also informal and to some degree affected by the pressures to start producing answers to our interoperability standards questions. As a result, we sacrificed understanding within the industry about the process that was used and what its implications would be as we sit here today.

The formal consensus-building process we have in place today called the Smart Grid Interoperability Panel is a relatively recent development, while the process of selecting standards for recommendation to FERC was one of our first priorities and activities that began many months before the establishment of the SGIP. In short, we built the process we need to use for establishing consensus in parallel to selecting an initial group of standards for recommendation in the interest of saving time. However this same time-saving reaped from running efforts in parallel has also cost us in our ability to make claims in regards to the adequacy of consensus. Regardless, the process of designating consensus for these standards was not the same process as is used today, and even today's process may need more rigor and sophistication if it is to support the weight of regulatory rulemaking.

Fortunately for the standards under consideration, the IEC process is one of the most technically sound and mature for developing standards relevant to the electric power industry. With this maturity comes stability - an attribute that, when coupled with technical integrity, allows technology to develop to the point of providing a rich ecosystem of available solutions. However maturity and stability also come at some expense of agility, and today's cyber security realm moves quickly. This discrepancy requires specific attention when considered in the context of regulatory enforcement.

In particular, some of the cipher suites specified in IEC 62351 need to be updated to reflect recent changes in the cyber security landscape. Cyber security research tends to operate like age and use on a rigid structure: fissures (or failures) tend to appear without warning and go to unpredictable depths. A cipher suite may go for decades without any significant attack, then suddenly encounter an assault that immediately compromises its use - sometimes partially and sometimes fully. This characteristic fundamentally distinguishes cyber security requirements from business requirements. Therefore, any reference to cyber security standards must provide a means to accommodate change and transition. This is an area where we cannot be too prescriptive, and must allow standards to evolve with advancements in technology.

This need to allow for evolution and advancement takes on special meaning in the environment of utility operations. The utility's fiduciary responsibility to ratepayers, commissioners, and sometimes shareholders dictates that decisions are considered very carefully and frequently drives technology to long deployment lifecycles. Utilities must develop strategies that allow for ongoing change in security technology and provide means to address legacy equipment concerns. Binding utilities to a frozen snapshot of an evolving standard will ultimately hobble innovation and force systems to expose vulnerabilities. We do not want to compromise tomorrow in our haste to find a solution today.

Today and for tomorrow, the industry needs a publicly visible process that delineates each step along the way from nomination of a standard to rulemaking. If we are to understand the implications of our

Statement of Darren Reece Highfill
Founder, UtiliSec
January 31, 2011

decisions at each step along the way, we must be able to trace the lines out through the end and back around to the beginning. The processes established in the SGIP represent a worthwhile first attempt to address a slice of this cycle. These processes need refinement, and even more importantly, we need to understand what happens after the SGIP.

In light of the questions raised by FERC for this conference, we would do well to consider the meaning of the terms “consensus” and “adoption” in this environment. Specifically, we need to ask the question, “consensus to what end?” The five IEC standards recommended by NIST are extremely detailed, highly prescriptive technical specifications, down to the point of directing which bytes go where in electronic packets on the wire. What are the implications of mandating this level of prescription through rulemaking? What happens when we mandate a standard that seems adequate today but turns out to need an immediate update tomorrow? How do we use regulation to protect the safety and security of customers against a rapidly moving adversary in a constantly changing landscape? Who owns the process for updating a standard?

I recommend the Commission carefully consider these questions prior to making any decision about implementation of the five IEC standards recommended by NIST. We need engagement between those that understand technical law and those familiar with the implementation of such standards in the real world. We need a transparently defined process that illustrates how detailed, implementation-specific standards can be updated within the context of regulation. I further recommend the Commission work with NIST and industry to produce a detailed lifecycle depicting the process for industry engagement, achieving consensus, relevant rulemaking, and subsequent assessment.

In summary, the five IEC standards recommended to FERC by NIST are helpful and powerful in their own right, but potentially dangerous tools in the context of regulation if not implemented properly. We must address concerns regarding the procedure for arriving at consensus to ensure we maintain industry and consumer confidence, and be exceptionally mindful to allow for resolution of technical standards issues essential to maintaining the long-term operational integrity of regulated utilities. Both the industry and the standards must invest the time and effort to come together on technical issues, cultivate fair and transparent processes, converge on appropriate use and implementation, and find a way to evolve and change together.

Respectfully submitted,

Darren Reece Highfill
Founder, UtiliSec

113 Greywood Place
Oak Ridge, TN 37830
(865) 806-8675
darren@utilisec.org