

FERC TECHNICAL CONFERENCE
The Smart Grid Interoperability Standards Process for
Reviewing and Selecting the First Five Families of Standards

COMMENTS BY GIB SOREBO, CHIEF CYBERSECURITY TECHNOLOGIST,
SCIENCE APPLICATIONS INTERNATIONAL CORPORATION (SAIC)

Introduction

I am pleased to provide FERC with written comments associated with my participation on a panel addressing the process of reviewing and selecting the First Five Families of Standards. Before I begin, I want to state that my comments are directed at cybersecurity and I am deferring to others on the interoperability details. However, I did want to address the wisdom of FERC endorsing standards of this nature from both an interoperability and cybersecurity perspective. To me, FERC's first priority should be to provide overarching guidance to ensure that utilities are implementing a comprehensive program that addresses interoperability and cybersecurity in all aspects of their smart grid projects. This was the intention of the guidance the Department of Energy mandated as part of the Smart Grid Grant program. Utilities had to provide a Cyber Security Plan as well as describe how interoperability goals would be met. Documents like NIST Interagency Report 7628, while still in draft form, are probably the best model for providing initial guidance. When combined with regulations like NERC CIP, utilities have good direction even if some of the details need to be addressed later.

Challenges with Endorsing These Standards

Moving forward with the Five Families of Standards would unnecessarily confuse utilities. I already have had customers ask whether they need to talk about how they comply with IEC 62351 in their Cyber Security Plans. Such an issue is far too granular to be discussed in the document. I would strongly urge the commission to provide more comprehensive guidance. In my opinion, all parts of a utility should comply with NERC CIP¹ at some level. That control framework is largely consistent with security best practices across multiple industries. And while technical feasibility exceptions will be needed, the growing sophistication of smart grid technology means that smart grid components effectively address NERC CIP requirements right out of the box.

As I noted, the Five Families of Standards is not appropriate as broad-based guidance for cybersecurity. In fact, only one, IEC 62351, devotes a significant amount of attention to cybersecurity. Rather than recommend these standards at face value, I would suggest that they be treated as procurement guidance. For example, NIST² could develop a smart grid procurement guide addressing interoperability and cybersecurity issues that would map recommended requirements for particular applications (e.g., control center to control center communication, substation automation, distribution management systems, energy management systems) to specific standards for different parts of an infrastructure. Such a document would be easier for vendors, utility procurement officials, managers, and

¹ CIP – Critical Infrastructure Protection ²NIST – National Institute of Science and Technology

engineers alike to refer to as needed. The “Smart Grid Interoperability Panel – Cyber Security Working Group Standards Review Phase 1 Report (October 7, 2010)” is written at a highly technical level that is hard to follow. Utilities need guidance and not exhaustive analysis of an abstract standard. As it stands now, a FERC decision to endorse these standards would leave many utilities with no choice but to purchase the standards to determine where they apply and where gaps need to be addressed. Asking them to spend thousands of dollars to purchase standards that may not be even relevant to what they’re doing is likely to lead to more confusion and frustration. While these standards are potentially useful, the commission needs to ensure that the guidance is targeted and includes easy-to-understand explanations that describes how the standards are to be used and for what purpose. The current NIST document does not do that.

The Standards Evaluation and Endorsement Process

My involvement with the standards subgroup that evaluated these standards was limited. While I was technically a member of the subgroup, other commitments prevented me from devoting much time. Consequently, I am relying on the documentation generated through e-mails, minutes, spreadsheets, and reports to assess the overall process. I would first like to acknowledge the dedication of the active members of the subgroup. They devoted significant time and energy to this activity voluntarily and should be commended for their efforts. However, my concern is that the process followed is inconsistent with what FERC is considering here. Specifically, the process did not define evaluation criteria to determine whether cybersecurity is sufficient for the standards. Instead, the report and prior discussions focused on identifying areas where cybersecurity is addressed and where gaps are found. This is a very useful exercise, but it does not provide sufficient information for FERC to endorse or recommend these standards from a cybersecurity perspective.

While it may be true that these standards are important for implementation of the smart grid, and some, such as IEC 60870-6, have already been in use for decades, it seems a bit random to pluck out five standards and declare them ready for deployment. While I may not be privy to all the discussions involved in this selection process, it is less than clear that evidence supports a formal FERC endorsement. Moreover, I question the value of FERC getting involved in endorsing these specific standards. Even though the endorsement would not constitute a requirement that utilities or vendors adopt these standards, other regulatory bodies may seek to make these voluntary standards mandatory. That creates other challenges such as the lack of sufficient audit criteria to verify compliance with the standards as well as any guidance on what extensions to these standards may be permitted. As threats change, it is important that product vendors keep cybersecurity features current. The application of mandatory standards could slow that process down.

Conclusion

For the above reasons, I recommend that FERC not take any action on these standards but instead emphasize its longstanding support for interoperability and cybersecurity for both

standards and their eventual implementation. FERC should further emphasize the importance of NERC CIP to cybersecurity for the electric grid, including smart grid applications, and should encourage all utilities to adhere to its requirements to the greatest extent possible. Additionally, FERC should encourage NIST to continue its critique of the various smart grid standards to promote cybersecurity and interoperability but should refrain from endorsing specific standards absent a compelling need to do so.