Opening Statement to FERC Technical Workshop
Andrew Wright

January 31 2011

I have been involved in NIST's CSWG since its inception in the spring of 2009, and to a limited degree in some other efforts of the SGIP. I proposed and co-led the Bottom Up Analysis subgroup of the CSWG that developed section 7 of NISTIR 7628. Consequently I have been reasonably involved and informed in the work of the CSWG throughout its entire process.

It is my opinion that there has not been sufficient consensus to consider the five families of standards posted by NIST as ready for Commission consideration in a rulemaking proceeding. I offer four points, most of which focus on cyber security, since that is my area of expertise.

1. What consensus process?

I have been involved in the SGIP and the CSWG since their inception. I was never aware of the initiation of any public consensus process that would lead to posting of standards for FERC consideration. I recently asked about a dozen colleagues, many of whom have also been involved in the NIST effort, and excluding NIST employees, none of them knew about any such process either.

2. There are serious cyber security problems with the standards.

The cyber security reviews of these standards performed by the CSWG identified a number of serious problems with the ones that address cyber security. Some of the problems are due to use of outdated cryptography - per recommendations from NIST's Computer Security Division. Some of the problems are due to references to outdated IETF standards. Many of these problems appear to have been outstanding for several years. Even if the standards can be fixed to address these problems quickly, this leaves the problem of ensuring that they continue to be updated on a timely basis as the IETF standards and NIST cryptography recommendations evolve.

3. The standards under consideration have significant limitations to access, primarily in the form of costs and license requirements. These limitations to access discourage open review that might otherwise uncover cyber security vulnerabilities.

Designing algorithms and protocols that operate correctly and are free of undiscovered flaws is difficult at best. There is general agreement in the security community that openly published and time-tested algorithms and protocols are less likely to contain security flaws than those held in secrecy, because their publication enables scrutiny by the entire community. Limitations on access to standards may pose challenges to smaller commercial entities implementing Smart Grid products, solutions, or systems. But in addition, these limitations may discourage inspection and review by security researchers, academics, and other interested parties, and may thereby increase the risk that Smart Grid standards contain security vulnerabilities.

While the standards under consideration are open in the sense that anyone can gain access to a standard, they are not as open or freely accessed as the IETF and W3C standards that define the Internet and that can be downloaded free of cost and restrictions. The standards NIST has recommended must be purchased from the Switzerland-based IEC organization, and a complete electronic set of these standards costs 10,738 Swiss Francs, or about $11,000 USD. Furthermore, purchase requires agreement to a license that restricts use of the standard to one person.

NIST recognized that financial costs alone would impose a significant barrier to NIST's own review, and negotiated special access through a web portal for a limited number of people within the CSWG to review standards. The IEC standards became available through this portal about May of 2010, but became unavailable about October of 2010 in the transition to a new portal, and as of January 21 were still not available on the new portal. Consequently, any member of the CSWG whose interest in reviewing the IEC standards was elevated by the announcement of the NIST posting has been unable to do so using this access.

4. There has been insufficient consideration of relevant cyber security standards, technologies, and best practices outside of the realm of power system standards.

The standards under consideration address some aspects of cyber security; however, they do not provide comprehensive coverage. A number of common IT security standards, technologies, and best practices can significantly contribute to security in practical deployments of these standards. NIST's own PAP1 effort identifies several such standards and technologies, including IPSEC, TLS, MPLS, and firewalls. I would add to these standards such as SSH, RADIUS, and LDAP; technologies such as intrusion detection and network access control; and best practices such as NIST SP800-53, SP800-82, and SP800-64. These time-tested standards, technologies, and best practices are in wide use today to secure corporate desktops and networks, branch office connections, web commerce, Internet banking, and many other critical applications. Where applicable, their use can significantly reduce cyber security risks with deployments of new technologies utilizing Smart Grid standards. With the exception of PAP1, the NIST and SGIP processes have largely neglected these standards, technologies, and best practices that address critical issues in securing the collection of systems that will form the Smart Grid. A FERC rulemaking that accelerates adoption of Smart Grid standards without requiring associated use of existing relevant cyber security standards, technologies, and best practices risks reducing the reliability of the grid.

Thank you.