

Comments on the *FERC Notice of Proposed Rulemaking, Mandatory Reliability Standards for Critical Infrastructure Protection*
Published in the Federal Register on August 6, 2007 in Docket RM06-22-000
October 5, 2007

By

Stuart W. Katzke, Ph.D.
Senior Research Scientist
National Institute of Standards and Technology
100 Bureau Drive; Stop 8930
Gaithersburg, MD 20899
skatzke@nist.gov
(301) 975-4768

And

Keith Stouffer
Senior Mechanical Engineer
National Institute of Standards and Technology
100 Bureau Drive; Stop 8230
Gaithersburg, MD 20899
keith.stouffer@nist.gov
(301) 975-3877

These comments are in response to your solicitation for comments on the *Notice of Proposed Rulemaking, Mandatory Reliability Standards for Critical Infrastructure Protection* of July 20, 2007 (hereafter referred to as the “**NOPR**”). The NOPR reflects FERC’s consideration of comments received on the *Federal Energy Regulatory Commission (FERC) Staff Preliminary Assessment of the North American Electric Reliability Corporation’s (NERC) Proposed Mandatory Reliability Standards on Critical Infrastructure Protection* (hereafter referred to as the “**NERC CIPs**”)

In our February 6, 2007 response the *Federal Energy Regulatory Commission Staff Preliminary Assessment of the North American Electric Reliability Corporation’s Proposed Mandatory Reliability Standards on Critical Infrastructure Protection* issued December 11, 2006 in Docket RM06-22-000, we indicated that:

“Our assessment is that the NERC CIPs do not provide levels of protection commensurate with the mandatory minimum federal standards (FIPS) prescribed by NIST (in FIPS 200 and NIST Special Publication 800-53, Revision 1 (hereafter referred to as **SP 800-53**)) for protecting federal non-national security information and information systems, including industrial control systems (ICS), from cyber attacks. As you know, ICSs are pervasive through the bulk electric system, as well as all other critical infrastructures. Since there are federal

agencies that operate and/or have control over the operation of ICSs that support the bulk electric system, these agencies must meet NIST standards and guidelines as well as standards required by FERC for these ICSs. To assist these agencies, NIST is developing an interpretation of SP 800-53 that is specific to ICSs. The ICS interpretation will be available in 2007 for use by federal agencies in demonstrating their (partial) compliance with the Federal Information Security Management Act of 2002 (FISMA). The ICS interpretation of SP 800-53 will be available for use by the private sector on a voluntary basis.

Our recommendation is for FERC to consider issuing interim cyber security standards for the bulk electric system that:

- Are a derivative of the NERC CIPs (e.g., NERC CIPs; NERC CIPs appropriately modified, enhanced, or strengthened), and
- Would allow for planned transition (say in two to three years) to cyber security standards that are identical to, consistent with or based on SP 800-53 and related NIST standards and guidelines (as interpreted for ICSs). This will be a plan to strengthen the NERC CIPs, rather than a plan to abandon them.”

In preparing our comments (below) to FERC’s NOPR, we have taken into consideration:

1. The recent disclosure of the Aurora Generator Test (<http://www.cnn.com/2007/US/09/26/power.at.risk/index.html>) and
2. NIST’s case study of the 1999 Bellingham, Washington Pipe Rupture event (<http://csrc.nist.gov/groups/SMA/fisma/ics/documents/papers/Bellingham-Case-Study-briefing.pdf>). In that case study we pointed out that implementation of the NIST Moderate baseline of security controls may have reduced vulnerabilities in the Bellingham control system that were relevant to the cyber event. While it is not possible to predict if the additional controls would have prevented the cyber event because of the many factors that contribute to such an event, it is clear that implementation of the NIST control set would have resulted in stronger protection of the Bellingham ICS.

Comments:

While we compliment FERC for proposing a derivative of the NERC CIPs that is an improvement over the original NERC CIPs (e.g., in the areas dealing with technical feasibility, risk acceptance, business interests), the proposed NOPR still falls short of meeting the federal minimum standards (i.e., FIPS 200 and NIST SP 800-53) for all federal non-national security information and information systems, including industrial control systems (ICS) owned/operated by the federal government. We point out that the proposed NOPR will leave information systems that support private sector bulk electric power systems less protected than comparable federal information systems`. Furthermore, it should be noted that the federal standards mandate minimum controls

(emphasis on *minimum*) as a starting point for determining the controls necessary to protect an information system. For Moderate and High Impact federal information systems (we believe most bulk electric information systems would be in these categories), we expect that, based on additional risk analyses, additional controls would be necessary to supplement the mandated minimum controls in order to provide acceptable levels of risk against a determined attacker. Consequently, we suggest you consider strengthening the starting point of the NERC CIPs that you propose in the NOPR.

With regard to our second recommendation, we would have liked to see FERC propose a more definitive transition strategy to stronger cyber security standards. The NOPR indicates that FERC “expects the ERO to seek and consider comments from those federal entities on the effectiveness of the NIST standards and on any implementation issues. Any provisions that will better protect the Bulk-Power systems should be addressed in the ERO’s Reliability Standards development process.” In concluding that section of the NOPR (Paragraph 88), FERC indicated that it “may revisit this issue in future proceedings as part of an evaluation of existing reliability standards or the need for new Reliability Standards, or as part of addressing NERC’s performance of its responsibilities as the ERO.”

On July 13, 2007, NIST released the ICS augmented version of SP 800-53 for public comment (the public comment period closed on August 31, 2007). To date, we have received no “show-stopping” comments concerning the effectiveness of the NIST standards and implementation issues from federal agencies, or from the private sector. Based upon the public comments we did receive, we expect that the ICS augmented version of SP 800-53 will become final by the end of the calendar year. Furthermore, FERC should be aware that there are significant efforts underway by the DoD and the Intelligence Community to make NIST’s security standards the foundation for the entire federal government. In light of the above, we suggest FERC reconsider its proposed position with regard to a transition strategy and propose a transition strategy, including timeframes, that moves the protection level of information systems that support the bulk electric power community from those proposed in the NOPR to cyber security standards that are identical to, consistent with or based on SP 800-53 and related NIST standards and guidelines (as interpreted for ICSs).