

**PREPARED STATEMENT OF ANDREW A. BOCHMAN  
ENERGY SECURITY LEAD, IBM/RATIONAL**

**BEFORE THE  
FEDERAL ENERGY REGULATORY COMMISSION**

**TECHNICAL CONFERENCE ON  
SMART GRID INTEROPERABILITY STANDARDS  
31 JANUARY 2011**

## Opening Remarks

Good afternoon, Chairman Wellinghoff, Commissioners, staff and all involved. I want to thank the Commission for convening this conference and for the opportunity to provide a few remarks.

I'm Andy Bochman, a former Air Force communications and computer officer, veteran of several cyber security start-up companies, and today am the Energy Security Lead for IBM Software Group's Rational Division, which focuses on software tools. Here we work to ensure that the software out of which the Smart Grid is being constructed is secure.

I've also been a blogger on energy topics since 2004 including the Smart Grid Security Blog (<http://smartgridsecurity.blogspot.com>) and DOD Energy Blog (<http://dodenergy.blogspot.com>), and a member of government and industry working groups including NIST's Smart Grid Cyber Security (CSWG), and the Grid Wise Alliance group on Smart Grid Interoperability and Security

With FERC poised to recommend these standards for consideration, there's a distinct possibility that State Public Utility Commissions (PUCs) and other regulatory organizations might quickly promote them to fill what they see as a void in guidance. But I ask you to consider the activities that led to the development of these draft standards a thorough learning and warm-up exercise that puts us in excellent position to now get it right.

Actually, this is my main point. As this panel's task is to consider and comment on the future of these processes, I suggest we allow enough additional time going forward to do two things: 1) to adjust how we do this job based on what we've learned to date, and 2) to set future milestones that are aggressive, but not so aggressive that the quality of what we build suffers.

I will now touch on some of the topics we were asked to consider:

How changes to existing NIST processes for identifying standards for consideration will promote: information sharing, transparency and consensus development.

AB: My experience with this standards development process has been that it provides all three of these desirable attributes in abundance. Community members have as much access, and as loud a voice, as their time, energy and experience allow.

Role of the SGIP committees and working groups in providing input for development and identification

AB: It seems to me that providing thoughtful input is what these groups are all about. I've had direct experience with the CSWG and some of its sub-groups, have participated in conference calls and reviewed drafts. It's amazing how dedicated these teams of experts are at getting the standards fleshed out as quickly, accurately and comprehensively as possible.

#### Miscellaneous

AB: The time and expert human capital required to do this work well are substantial. The standards before us today have not had nearly enough cyber security scrutiny as evidenced by the fact that experts and informed laypersons alike have found glaring security problems with them. Regarding legacy integration, I'd like to cite this warning from Erich Gunther, Founder and CTO of Enernex, something I included on my blog in 2010:

*One must keep in mind that there will be far more poorly coded, totally untrustworthy firmware and software in the field for decades (that's the existing installed base) than new, more secure systems following sound development practices installed over the same time period. Dealing with this reality and the fact that the old stuff will not be ripped out should be a priority.*

Lastly, my interactions with them reveal that power industry cyber security professionals have a wide range of familiarity with the SGIP and other security-related standards, with many dozens of highly skilled practitioners leading the way at our larger utilities, but with diminishing expertise and capabilities in smaller organizations.

In addition to these, here are three additional cyber security issues related to the five foundational standards and others that merit greater attention in the near-term:

- Implementation of measurement/metrics for cyber security controls across the grid and Smart Grid
- Greater emphasis on lab testing of new and updated products. And as Stuxnet showed us, we need greater attention to supply chain security issues
- Better forensics and preparations for recovery from successful cyber attacks by utilities and regional operators

It's been an honor and a privilege to be a part of the community imagining and developing guidance for the future grid. While the interoperability and cyber security challenges are formidable, I believe the Smart Grid's rewards greatly outweigh the risks. Given more time, I believe we have in us, collectively, the experience and expertise to craft guidance and standards that will ensure very strong outcomes for the grid and the nation. And FERC's willingness to hear from the industry's developers is a good indicator that the results will be positive.

Respectfully submitted,

Andrew A. Bochman  
Energy Security Lead  
IBM/Rational

1110 Beacon St, #1C  
Brookline, MA 02446

Cell: 781 962 6845  
Email: bochman@us.ibm.com