

**PREPARED STATEMENT OF DANIEL THANOS
CHIEF CYBER SECURITY ARCHITECT OF GENERAL ELECTRIC DIGITAL
ENERGY.**

**BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION**

**Technical Conference on
SMART GRID INTEROPERABILITY STANDARDS**

January 31, 2011

I want to start by thanking Chairman Wellinghoff, Commissioners, officials, and all of the staff involved for the opportunity to speak at the technical conference for smart grid interoperability standards and putting the technology in place to allow it to happen. I would also like to thank the SGIP governing board, NIST CSWG, and GE for allowing me to dedicate considerable amounts of time to this and another important efforts. Most of all I would like to thank my wife Isel, she allows me to donate large amounts of our personal time because she believes in me and this work that I see as my mission.

As my video is coming to you live from the Internet, whose performance we do not control, I ask your patience if there is any temporary losses of image, my audio will continue over the teleconference bridge. The views and opinions that I will communicate are my own; they do not necessarily represent those of my organization.

It has been a real honor and privilege to work with people across many different private and public sector organizations with a diversity of technical and professional backgrounds in the process of helping form the NISTIR 7628 Guidelines for Smart Grid Cyber Security. I feel fortunate enough to have learned from my work in the various CSWG subgroups as much as I have contributed. The voluntary work that went into developing the NISTIR for the scope of systems and rapid time frames involved has been monumental. It has been a true testament to the hard work and expertise of the whole CSWG volunteer core and the leadership of the group, and I believe it is a model for how innovative public-private initiatives should work. It is that hard and innovative work I am here to represent and preserve for the good of the public and broader industry. In that spirit I also wish to make sure that the good standing and reputation of all stakeholders involved is continued and that is the basis of any critical analysis I have to offer in the standards review process. I would also like to state that I have a high regard for the entire panel, and I have immensely enjoyed working with all of them.

I am sure everyone has had a chance to read panelist biographies and realize there is an excellent depth of knowledge and expertise that will be heard from, I am just a small part of that. Thus I will not dedicate much time on my background beyond giving a context of my involvement in the NIST effort and the industry. I helped co-lead the following NIST CSWG subgroups: BU technical analysis, R&D, and Cryptography and Key Management. I also contributed to many of the other subgroups. I am involved in IEEE, OpenSG, NERC, DHS, and IEC working groups engaged in developing security best practices/guidance and standards. I continue to be very engaged in the CSWG where I co-lead (with Annabelle Lee) the newly formed Design Principles Group that will work to show how to apply the NISTIR at a practical and technical level. In my role for GE I am deeply involved in researching, designing, and developing security hardware and software technologies for a broad range of automation and communication systems and devices. My perspective comes from someone that has to build the technology and ensure it can be reliably operated by a very large and globally distributed customer base in Smart Grid and other critical infrastructure industries. Thus I understand very well the need to make principled and sound decisions at this critical juncture. I also equally understand that for sake of continuing to increase security and reliability in the Smart Grid we must be solution focused in how we move forward with accepting the standards in question. I am here to try to offer a balanced view and be part of the process of solving the problems that are needed to keep industry momentum moving forward.

The NIST standards review process was taken up by very dedicated and hardworking volunteers who we should all thank as they were asked to perform considerable amounts of work under aggressive time lines. My views are in no way meant to detract from their dedication and work. However, I do have concerns with declaring the review work that has been completed thus far as final and sufficient to garner total acceptance of the standards under consideration. This work was a start and it has identified issues that simply need to be addressed as acceptance without a solution for correction would cause confusion and hamper the trust and reputation that has been vested in all the organizations involved. This is because there are fundamental security errors in the standards and confused concepts when trying to give informational backgrounds for various security terms and technologies. There is also need of an update to the standards to reflect the work of the NISTIR with special attention to the cryptography requirements. Time does not allow me to make this a forum to discuss each issue, nor is that needed as all parties involved are aware of them, and you can find some in the NIST standards review reports, and I touched on them in my presentation in the last FERC technical conference. As I have discussed in the previous FERC technical conference on the adoption of these standards, there is a need for a more broad and open analysis of the standards in question especially by members of the security community. Also the underlying process and criteria that reviews are done under need to be improved and more formalized to allow for less interpretation and stricter evaluation against the NISTIR itself. I also believe there needs to be a better functional and system context by which these standards are evaluated. To this end there still continues to be some debate and evolution of the criteria which is used to evaluate the standards. While this is good and we are all trying to learn in this process, it is clear that because the criteria has not been finalized and broadly accepted that we need to address this before standards can be deemed to meet the needed requirements. I hope this conference provides valuable input for the purpose of developing those criteria. Lastly standards have normative references to other standards, which in turn may reference other normative standards, it is not clear how detailed these references have been reviewed if at all, yet they may also be accepted in the process. That should cause us some pause while we also make sure that referenced standards are indeed the best most current ones to use. There are instances where this is not the case and this also needs to be addressed.

What is important to emphasize and work on now is the fact that none of these mentioned problems are intractable and without a straight forward solution. We only need the will and leadership to get it done. Depending on what solution path is taken there might be a relatively expedient resolution. To that end what I recommend for the acceptance of the current IEC standards is the development of a correcting and overriding security addendum that must be adopted along with the standards. I believe this would address all concerns. The addendum would correct all errors, reference the most current and secure standards, and provide any needed modifications to meet NISTIR requirements. The addendum should be developed under an open process and ensure review by all needed technical experts. Alternatively we could require the standards development groups to revise the standard per addendum before it is accepted, but this maybe a considerably longer process. In parallel to addendum development the standards review process needs to improve and introduce more phases and rigor as to give better assurance of clarity, consistency, and broad acceptance. I look forward to discussing these and other topics with the panel.