

Statement for the Record, July 21, 2009 Hearing before the Subcommittee on Emerging Threats, Cybersecurity, Science and Technology

Darren Reece Highfill

AMI-SEC Task Force and UtiliSec Working Group Chair, UCA International Users Group

The Advanced Metering Infrastructure Security (AMI-SEC) Task Force along with many of its sibling activities in the UCA International Users Group plays a critical role in our nation's efforts to secure the smart grid. To date, no other organization has produced guidance as timely, targeted, technical, and widely accepted for smart grid security as AMI-SEC. The AMI-SEC Task Force and its immediate parent group, the UtiliSec Working Group, are currently working feverishly to extend this work and make it more usable by the entities at the heart of this process – electric utilities and the vendors of smart grid equipment and services that support them. The problem at hand is extraordinarily complex, and continued support of public-private partnership projects is essential to development of effective guidance that will in turn enable the lights to stay on, provide the nation with assurance of secure and proper implementation, and allow the smart grid to become a reality.

The AMI-SEC Task Force is a part the UtiliSec Working Group, which is responsible for developing security requirements for all smart grid applications for the UCA International Users Group (UCAIug), a 501(c)(3) non-profit corporation supporting members of the electric utility community in efforts to promote, adopt, and implement open and public standards for industry-specific communications technology. The UCAIug has well over 100 corporate members from 29 different countries, along with hundreds of “friends of the UCAIug” – people who subscribe to various list servers and participate in our meetings, but have yet to formally join the UCAIug.

Both AMI-SEC and UtiliSec now reside in a family of activities within the UCAIug referred to as Open Smart Grid, or simply OpenSG. The utilities that actively participate in OpenSG are some of the largest in the United States, and collectively represent over one quarter of the residential meters in the U.S. OpenSG is focused specifically on development of industry requirements for smart grid communication technologies, and includes such groups as UtilityAMI, OpenHAN, AMI-Enterprise, UtiliSec, and AMI-SEC in addition to several others. However, this momentum took some time to build.

The AMI-SEC Task Force was formed in August of 2007 as a part of UCAIug efforts to define requirements around the rapidly evolving advanced metering infrastructure (AMI) space. By the end of 2007, AMI-SEC had gained significant following and generated strong technical analyses of AMI security issues, but was also under increasing pressure by industry to produce actionable guidance for AMI systems in development. Utilities and vendors alike at the forefront of this issue understood the need for security in the AMI domain.

In January 2008 AMI-SEC delineated a set of deliverables for calendar-year 2008, including a set of requirements for development and implementation of secure AMI systems. The production of these requirements involved substantial supporting research. While volunteers put forth valiant effort on the first task, the leadership recognized that the pace was not sustainable. As the task force volunteers neared the first milestone it became apparent that decreasing resource availability and an increasing number of demands from other projects would prevent AMI-SEC from reaching its goals.

A few leading utilities including Southern California Edison and Consumers Energy recognized the significance of the developing issue, and offered to commit dedicated resources and funding to a collaborative project to help get the work done. Still, the effort would require broader representation and investment by the utility community, so the AMI-SEC leadership framed an opportunity description and began to solicit additional utilities for support. The AMI-SEC leadership also reached out to Hank Kenchington in the Control Systems Security Program at the U.S. Department of Energy, who expressed sincere interest in helping utilities secure this nascent set of assets. The Electric Power Research Institute as well offered support, quickly turning the opportunity into a powerful collaboration.

The opportunity became the original AMI Security Acceleration Project (ASAP) – a powerful collaboration between the U.S. Department of Energy, the Electric Power Research Institute, and a dozen of North America's largest electric utilities, including American Electric Power, Austin Energy, BC Hydro, Consumers Energy, Dominion, Duke Energy, Exelon, Kansas City Power & Light, Oncor, Pacific Gas & Electric, San Diego Gas & Electric and Southern California Edison. ASAP brought together utility domain experts, private sector security engineers, and resources from Federally Funded Research and Development Centers such as Oak Ridge National Laboratory, Idaho National Laboratory, and the Software Engineering Institute at Carnegie Mellon to perform the arduous work of content development for AMI-SEC. Over the course of the next six months, the team produced mature drafts of each of the remaining AMI-SEC deliverables, including the AMI System Security Requirements.

Each of these deliverables was subsequently handed off to the AMI-SEC Task Force for review, commentary, editing, and approval. The AMI System Security Requirements were unanimously approved by members of the task force in December of 2008, and the document was published with a "1.0" designation. The document laid the foundation for securing the smart grid by thorough analysis of the emergent field communications and control issues brought about by AMI. The AMI System Security Requirements built on numerous public and private sector security best practices documents, and aggregated a large and heterogeneous set of security controls into a single homogenous resource for the procurement of secure AMI technologies.

The AMI System Security Requirements however do have room for improvement. Detailed examination of the AMI System Security Requirements by the broader technical community brought compliments for its completeness and rigor, along with a notable complaint about its usability. While the document is technically sound, it is also sizeable and dense, and not necessarily easy for organizations to determine which parts applied to them without considerable effort to absorb and understand the entire publication. Additionally the industry now needs guidance for securing other smart grid applications besides just AMI. Distribution automation, wide area situational awareness (synchrophasors), substation

automation, remedial action schemes, and outage management are but a few aspects of the smart grid that are crossing a key threshold of adoption or integration. Each of these will need commonly accepted requirements for security that utilities and vendors may agree upon and reference.

In response to this rapidly growing landscape of technologies needing security guidance, OpenSG formed the UtiliSec Working Group to develop detailed security and assurance requirements and security best practices guidance for organizations throughout the lifecycle of smart grid technology. The AMI-SEC Task Force was moved under the UtiliSec Working Group as part of the associated re-organization, and the bulk of the work shifted to the UtiliSec Working Group level.

With the recent success of the AMI Security Acceleration Project and a growing list of tasks, the UtiliSec leadership promptly assembled a follow-on collaborative opportunity called the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG). ASAP-SG's technical objectives are two-fold: expand the AMI-SEC guidance to other applications for the smart grid, and improve the ability for users to approach, understand, and implement the guidance for securing smart grid systems. At the same time, ASAP-SG has quickly become a mechanism to synchronize efforts of the UtiliSec Working Group with the complimentary activities of the National Institute of Standards and Technology (NIST) in development of an Interoperability Framework for the smart grid. Specifically, the NIST Cyber Security Coordination Task Group (CSCTG) and UtiliSec Working Group are working tightly together to develop guidance for security of the nation's smart grid, and ASAP-SG is means by which key pieces of the work are getting done and fed in to both organizations.

Like the original AMI Security Acceleration Project, ASAP-SG is a public-private partnership between electric utilities and the U.S. Department of Energy. The technical work is currently underway and DOE has brought substantial resources to the project. At the same time the private sector side has been partially funded by utilities, while project managers continue to work with additional utilities to align budgets and link funding mechanisms. Many of the same utilities that participated in the original ASAP are considering funding ASAP-SG, however Congressional stimulus funding opportunities have placed a significant load on utility personnel and it is sometimes challenging for utilities to find the appropriate level of prioritization for this project among many other current and timely opportunities.

Even after ASAP-SG is fully funded and completes the current set of deliverables, the industry will face many more challenges ahead. The original ASAP attempted to engage the AMI vendor community in independent third party vulnerability testing, and met unsuccessfully with an array of complications and challenges around intellectual property and the sensitivity of test results. The essential work of third party vulnerability testing is nonetheless going on now, but through isolated, singular, one-on-one agreements. No standardized, common approach or environment exists for vulnerability testing, and more importantly, neither does an effective process by which vendors and utilities can openly share critical vulnerability information in a community dialog.

The power industry is also working to find a way to effectively and consistently communicate with elements of the security research community. While many researchers approach the vulnerability disclosure issue by trying to work with the vendor, sometimes communications are difficult to establish

or the parties cannot agree upon appropriate responses and time windows. Unfortunately the rogue elements of the community sometimes respond by presenting their findings in unstructured and problematic manners. Legal efforts to dissuade this activity are frequently ineffectual and often backfire, in the end creating many more communication problems and adding to an already complicated dynamic. Ultimately the industry needs a means to address vulnerabilities that entices both security researcher and vendor to participate. Mechanisms like US-CERT exist that solve part of the problem, but to date no industry has found a way to resolve all concerns and bring all parties to the table.

Many utilities and vendors alike would also like to see a means of certification for security. While attractive in concept, the issues of implementation and endorsement contain notable difficulties. Good security requires a holistic approach, as can be mathematically proven by an illustration of two secure sub-systems combined to inadvertently create a vulnerable whole. This complicates the certification of any higher level systems, as nested interdependencies can create scenarios that are impractical to evaluate. Additionally, the endorsement implications of a system security certification raise liability questions that may present a prohibitive barrier to entry and discourage creative exploration.

In conclusion, the leadership of the AMI-SEC Task Force and UtiliSec Working Group within the UCA International Users Group respectfully requests that Congress sincerely consider means to prioritize, fund, and encourage the issues of security for the smart grid. Public-private partnership projects are a proven means of coordinating the interests of both government and industry, and leverage the complimentary expertise of each party involved. Utilities and vendors alike are proactive in this space, but the problems are many and large, and all could use support.

Thank you for your consideration.