STATE OF CONNECTICUT
CONNECTICUT SITING COUNCIL

RE: IMPLEMENTATION OF SECTION 8 OF PUBLIC ACT NO. 07-242 AN ACT CONCERNING ELECTRICITY AND ENERGY EFFICIENCY	: : : :	**Docket #346**

July 29, 2009
BRIEF
Energy Security Risks & Considerations

JOEL N. GORDES
DBA ENVIRONMENTAL ENERGY SOLUTIONS (EES)

While the path has been long, EES has deeply appreciated the opportunity to participate in Docket #346 pertaining to energy security and offers this brief to recap and reinforce the EES positions pertaining to the docket in general and the White Paper of May 28, 2009 in particular. EES also appreciated the latitude displayed by the CSC in taking up the EES Motion to have the CSC reconsider the White Paper position on the topics of natural calamities, cyberthreats and reliability as intrinsic to any such docket on "security" in its most holistic sense. While officially no action was taken on the motion, due to lack of a second on a motion to consider the EES motion, the willingness of the CSC to cross examine EES to bring forth some of these issues was extremely gracious and, EES hopes, useful. In short, EES thinks the hearing played a highly valuable role in distilling the essence of its message. EES hopes the following points made during the hearing, particularly those during the cross examination of EES by the Council, provides some basis for clearer understanding of the direction EES sees for CSC's role going forward in undertaking its legislatively-mandated security role:

- While the CSC originally had an environmental charge, that changed in 2003 with PA 03-140 and again with PA 07-242, Sec 8 with the legislature mandating certain security-related responsibilities.

- Whether facing a terrorist attack or a natural calamity, the results can be much the same as are potential remedies to them in siting to include the planning, response, mitigation and recovery functions.

- Natural calamities may be used to mask or enhance the effects of terrorist acts and should not be excluded from considerations. The security of the populous should not be limited by artificial and inappropriate divisions.

- Physical damage can take place via direct attacks against facilities or a variety of cyber means. Attempting to separate the source of the physical damage to exclude one or the other as CSC has preliminarily attempted to do is near impossible with systems becoming more digitally-based and intrinsic to most physical portions of grid operation and economics. In its initial testimony of 11/25/08 at p. 3, lines 88 and 427 EES specifically cited electromagnetic pulse as one such physical threat that could incapacitate not only the grid but any device using semiconductors. Hearing of a Congressional subcommittee indicate this is a serious concern. Recently Congressperson Yvette Clarke, Committee Chair of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, has said the utilities have adopted a "head-in-the-sand mentality that seems to permeate broad sections of the electric industry."[1] (See **Appendix A** for news accounts of these Congressional hearings.)

- A holistic approach to "siting" should take into account not only the facility at hand but its effects and interactions on the grid as a whole within the interconnected and currently highly centralized system. The very act "to site" or "not to site" carries immense security repercussions.

- Adding transmission capacity to the grid may be subject to diminishing returns of resiliency as suggested by the National Science Council[2] rather than adding resilience under all circumstances as suggested by some utility personnel at the hearing.

- Redundancy, alone, does not offer resiliency unless it also takes place within a more decentralized system.

- Many of the ecological principles honed by the CSC have application to security considerations including diversity, interconnectedness, dispersion and redundancy;

- Some overlap or even redundancies of function by the CSC in concert with other agencies, may play a pivotally important role at some future point in recognizing a

[1] Bliss, Jeff. U.S. Lacks Defense From Nuclear Pulse, Official Says. Bloomberg News. http://www.bloomberg.com/apps/news?pid=20601103&sid=aW9tDFume0MU July 21, 2009.

[2] A direct way to address vulnerable transmission bottlenecks and make the grid more robust is to build additional transmission capacity, but there are indications that redundancy has a dark side (in addition to increased costs). The likelihood of hidden failures in any large-scale system increases as the number of components increases. Modeling techniques are only now emerging for the analysis of such hidden failures." (see, for example, Wang and Thorp, 2001). *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism. National Academy Press. Committee on Science and Technology for Countering Terrorism, National Research Council. p.302*. 2002.

weakness deemed "too unrealistic" at the federal level as was exactly the case on 9/11.

- A potential weakness of a too narrowly-focused view of siting duties might be a failure to not comprehend "not knowing what we don't know". [3]

- Overly narrowing the examination of what constitutes "security" falls into the inclination to "stovepipe"[4]. This means developing solutions to narrow goals ("siting" in this case) that are incompatible to or even to the exclusion of other considerations.

- None of the parties or Council should forget the caution offered by the Kean-Hamilton 9/11 Commission Report that: "We believe the 9/11 attacks revealed four kinds of failures: in imagination, policy, capabilities, and management."[5]

Suggestions

EES would like to offer some modest suggestions for CSC's White Paper to better aid CSC in formulating and carrying out its mission including energy security activities of one form or another:

- Conduct follow-on activities to better refine what the term "security" entails and to include physical damage via cyber means including electromagnetic pulse;

- Participate in state and federal-level security exercises (such as TOPOFF conducted in CT in April 2005) as an observer to gain further insights into the relationship of security to siting activities;

- Define the word "siting" in CSC regulations as no concise definition is provided on what this means and/or its boundaries.

- Then, define the word "security" within CSC regulations 16-50j-2a based on this docket as well as used by others such as the CEAB etc.

- Request when a new member is named to the CSC that he/she have some experience in security matters;

[3] This point was made in a 1999 speech at Columbia University in regard to observations by Professor Dennis Mileti former Director of the Natural Hazards Center at the University of Colorado. Oddly enough, this concept has more recently appeared in a 2007 best seller titled *The Black Swan* by Nassim Nicholas Taleb.

[4] http://www.doubletongued.org/index.php/dictionary/stove_pipe/ was partially used in this definition.

[5] The 9/11 Commission Report. Thomas H. Kean and Lee H. Hamilton et al. (W.W. Norton & Co. New York) July 22, 2004. p. 339.

- Continue to explore and pursue relationships between solutions common to both environmental and energy security as outlined on p. 4, lines 114-129 of the EES comments of June 22, 2009.

- Upon application by any entity for construction of a new facility in Connecticut, require they demonstrate they are in compliance with security reporting requirements to the NERC, FERC, NRC, etc.

- In CSC's role to "promote energy security"[6], request NERC to notify CSC of any non-conformities of companies operating within Connecticut and be advised of any penalties sanctioned.

- Deny approval of projects in Connecticut to those in non-compliance with federal security mandates unless such projects are required to meet such mandates.

- While it is unknown to what degree the CSC will be asked to examine aspects of the emerging Smart Grid, it would be prudent to expect some activity. Investigation should begin of what emergence of Smart Grid technologies may mean to the CSC mission including security aspects.

- Before elements of the Smart Grid are widely deployed, coordinate with federal and other state entities to ensure that security-related aspects are addressed.

- Provide oversight and control for siting of certain security aspects relating to Smart Grid technology.

Conclusion

EES appreciates the opportunity to have participated in this docket. In closing, we have our regulations, our checklists and other requirements issued by federal authorities to guard against the unexpected. Unfortunately, terrorists and others who might wish us harm do not subscribe to the same checklists when developing their methods to compromise the operation of something as economically vital and attractive a target as the electric grid. While some may look at any CSC role as being purely redundant to federal level efforts, the advantage of local command, control, awareness and responsiveness cannot be underestimated when it comes to security concerns which are the first responsibility of government in a democratic society.

[6] As mandated in PA 03-140.

http://www.bloomberg.com/apps/news?pid=20601103&sid=aW9tDFume0MU

U.S. Lacks Defense From Nuclear Pulse, Official Says (Update1)

By Jeff Bliss

July 21 (Bloomberg) -- The U.S. must do more to protect itself against blackouts and damaged electronics that would be caused by a nuclear bomb blast, said the head of a panel established by Congress to monitor the threat.

The current vulnerability of our critical infrastructures can both invite and reward attack if not corrected, said William Graham, chairman of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack.

Graham testified today before a House Homeland Security subcommittee considering legislation authorizing the Federal Energy Regulatory Commission to force power plants and other critical facilities to protect against computer attacks. FERCs rules would be based on intelligence gathered by the Department of Homeland Security and U.S. spy agencies. Several similar measures have been introduced in the House and Senate.

Graham said Congress must address the potentially catastrophic consequences of an electromagnetic pulse, which would occur if a nuclear bomb exploded 25 to 249 miles (40 to 400 kilometers) above the ground.

Rogue adversaries, including North Korea and Iran, possess and test high altitude missiles that could potentially cause a catastrophic pulse across the grid, said Representative Yvette Clarke, the New York Democrat who heads the subcommittee that was holding todays hearing.

Potential Damage

Pulses can cause equal or greater destruction than cyber attacks, said Joseph McClelland, director of FERCs Office of Electric Reliability. The federal government should have no less ability to act to protect against such potential damage.

U.S. and Soviet atmospheric atomic tests in 1962 led to failed street lighting systems, damaged cables and tripped circuit breakers from as far away as 870 miles (1,400 kilometers) from ground zero, Graham said.

Solar flares and storms that disrupt the Earths magnetic field also can cause a pulse.

Threats notwithstanding, electric utilities may not be classifying as many facilities as they should as critical in order to avoid boosting security there, according to an official of the North American Electric Reliability Corp. The nonprofit group oversees reliability for power systems providing electricity to 334 million people.

Only 31 percent of separate, non-affiliated utilities reported at least one critical asset, said Michael Assante, NERCs vice president and chief security officer, in an April 7 letter released today by the subcommittee.

Clarke said the statistic epitomizes the head-in-the-sand mentality that seems to permeate broad sections of the electric industry.

http://www.pcworld.com/businesscenter/article/168797/lawmakers_electric_utilities_ignore_cyber_warnings.html

Lawmakers: Electric Utilities Ignore Cyber Warnings

Grant Gross, IDG News Service

Tuesday, July 21, 2009 2:10 PM PDT

The U.S. electrical grid remains vulnerable to cyber and electromagnetic pulse attacks despite years of warnings, several U.S. lawmakers said Tuesday.

The electric industry has pushed against federal cybersecurity standards and some utilities appear to be avoiding industry self-regulatory efforts by declining to designate their facilities or equipment as critical assets that need special protection, said Representative Yvette Clarke, a New York Democrat and chairwoman of the U.S. House Homeland Security Committee's Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology.

"This effort seems to epitomize the head-in-the-sand mentality that seems to permeate broad sections of the electric industry," Clarke said.

The U.S. electric grid is an "obvious target" for enemies of the nation, and a major outage would affect all aspects of everyday life, Clarke said during a Tuesday hearing. "We simply cannot afford to lose broad sections of our grid for days, weeks or months," she said.

Despite years of warnings from lawmakers, electric utilities' efforts to secure themselves against cyber or electromagnetic pulse, or EMP, attacks seem to be lagging, Clarke added. During a three-year subcommittee review of electrical grid security, committee members and staff talked to hundreds of experts and read thousands of pages of studies, she said.

"They all reached one conclusion: The electric industry has failed to appropriately protect against the threats we face in the 21st century," Clarke said.

While the hearing mostly focused on cybersecurity, lawmakers also talked about the threat of an EMP attack on the U.S. An EMP is a burst of electromagnetic radiation, usually from a nuclear explosion. While such an attack may be unlikely, an EMP attack could shut down the electricity grid over a wide area and bring the U.S. to a standstill, some lawmakers said.

Representatives of the electric industry said they've worked hard to improve cybersecurity, and they share the lawmaker concerns about EMP attacks. The electric industry needs better information about how to protect against EMP attacks, said Steven Naumann, vice president of wholesale market development at Exelon, an electric utility.

Part of the problem with cyberattacks is that the U.S. government doesn't share enough up-to-date information, Naumann added. "In general, the North American gird is well-protected against cyberattacks -- at least those attacks that we know about," he said. "It's hard to protect against something you don't know."

Many electric utilities have taken significant steps in recent years to improve their cybersecurity, added Mark Fabro, president and chief security scientist at Lofty Perch, a control systems security vendor. The electricity grid will continue to converge with the Internet and that will introduce vulnerabilities, he added, but many utilities are working hard to improve security.

"We continue to witness excellent examples of effective cybersecurity activities from many entities, and observe progress that does not align with the popular opinion that the bulk power system is rife for total system compromise," Fabro said.

But several lawmakers said they're concerned that the electrical grid will become more vulnerable as its controls move onto Internet Protocol networks. "There is a massive computer espionage campaign being launched against the United States by our adversaries," said Representative Bennie Thompson, a Mississippi Democrat and chairman of the full Homeland Security Committee. "Intelligence suggests that countries seek or have developed weapons capable of destroying our grid."