STATE OF CONNECTICUT
CONNECTICUT SITING COUNCIL

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

January 8, 2008
Proposed Scope of Proceeding
for
Section 8, Public Act 07-242
Pertaining to Energy Security

JOEL N. GORDES
DBA ENVIRONMENTAL ENERGY SOLUTIONS (EES)

I. EES Vs UTILITY POSITION ON SCOPE OF PROCEEDING

EES believes the first responsibility of government is to the security of its citizens. In its letter of 10/21/08 seeking intervenor status with the Connecticut Siting Council (CSC), EES clearly stated its intention:

> …to provide an alternate, and perhaps more holistic, perspective to enhance the CT Siting Council's formulation of security-oriented policies, processes, procedures and considerations to provide safe, reliable, secure and resilient power to Connecticut's commercial, industrial and residential sectors.

Subsequently, EES filed its comments/testimony early in a demonstration of openness and good faith as stated below:[1]

> EES hopes that it sets a positive and serious tone for this docket. EES is taking this unusual step of early disclosure fully knowing this may disadvantage EES's position. The comments/testimony effectively provides information to the parties in answering the EES interrogatories should they care to adopt them. The early disclosure also provides a greater period for them to develop counter positions. EES's intent in doing this is in the public interest of providing some baseline definitions/concerns to promote dialogue on a critical topic.

[1] Letter of Transmittal to Comments/Testimony of 11/25/08

In that testimony EES went on to seriously address the issues within the context of the CSC's proposed Best Management Practices (BMPs), as requested, but noted language within that CSC request that appears to allow some degree of latitude to go beyond, namely:[2]

> The criteria presented in this guide should be evaluated by applicants in their initial filing as much as practicable. [emphasis added.]

EES, in its letter of transmittal to the first round of interrogatories went on to say[3]:

> As previously noted, these interrogatories are largely but not exclusively framed within the context of the Best Management Practices (BMPs) as requested by CSC. They seek to elicit information that views the grid not in isolation on a component-by-component basis but, rather, in a more holistic sense wherein equal attention is paid to the interaction(s) of each component upon the whole and resultant effects on grid security.

Unfortunately, contrary to this, CL&P and UI (collectively "the Utilities") and, to a lesser extent, CMEEC have elected to not only summarily dismiss the need for the CSC's draft BMPs as duplicative but also question the CSC's statutory authority to address the very points of investigation[4] listed in both the statute itself and the BMPs. In these comments (at p.2, last paragraph), the Utilities have conveniently neglected to include these points in bold font as critical matters as they did certain other words such as "siting". In doing so, they have chosen the narrowest of interpretations in regard to the word "siting" and neglect the responsibility of the Council set out in 16-50g which since passage of PA 03-140 includes the phrase "to promote energy security." This may even be construed to go to security issues attendant to "siting" rather than exclusively environmental concerns as had been true prior to that act. Indeed, since that is 2003 legislation, one might ask what the Utilities have done to prepare for compliance with the statutory "promote energy security" (whatver it means) prior to this time.

EES is confused when UI and CL&P quote this same statute citing plain language to provide the opinion (Joint Memorandum at p. 1) "there is no need for exploration of detailed technical issues on the design of the facilities or their vulnerabilities". EES respectfully disagrees with this opinion and sees in it an attempt to change the very rules of the game to dissuade the CSC from its original course and its responsibility to the legislature to investigate energy security within this docket. EES has answered the questions the CSC has posed and

[2] CSC DRAFT Best Management Practices. Page 1, paragaph 4.
[3] EES letter of transmittal to first round of interrogatories. 10/31/08
[4] (Joint Memorandum at p.5, para.1)"…including consideration of planning, preparedness, response and recovery capabilities."

believes the Utilities should be required to answer the same CSC questions rather than divert the direction of the docket.

Even in relation to the interrogatories submitted by EES, the Utilities responses repeatedly maintain, "This question does not relate to siting of facilities and is beyond the scope of this proceeding" in an attempt to force the narrowest of scopes. This reply also presumptuously usurps the power of the Council which has sole authority to make that pronouncement of "being beyond the scope". To restrict "siting" to the Utilities' own, narrow definition is merely an opinion. Little factual information in support of their opinions has been forthcoming.

What may be at the root of this disagreement is how to define the word "siting". In light of events of 9/11/01 and new legislative mandates such as PA 03-140, this may require some reexamination. One insight into the meaning of "siting" might be to examine a caution from the National Research Council (National Academies of Science, Engineering, etc.) They have stated in regards to building (one assumes "siting" comes as a prior step) transmission lines for congestion relief:

> 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).[5]

If one is to give any credibility to this statement by such a prestigious group, a prudent interpretation might take it to mean that the very act "to site" (or "not to site") and build a grid generation or transmission facility carries with it the ability to strengthen or weaken the security of the grid. This exemplifies the EES-suggested approach to examine grid security:

> … not in isolation on a component-by-component basis but, rather, in a more holistic sense wherein equal attention is paid to the interaction(s) of each component upon the whole and resultant effects on grid security. [6]

EES does not agree with the Utilities to change the rules of the game so that the docket becomes merely an informational session to discuss the efficacy of FERC/NERC/NPCC/ISO-NE and NIST's various standards. Ironically, however, there is dialogue within the FERC Staff

[5] *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.
[6] Letter of transmittal to first round of Docket #346 interrogatories. 10/31/08

Preliminary Assessment[7] of the NERC proposed Critical Infrastructure Protection (CIP) standards CIP-002 through CIP-009[8] that add credibility to the need for a more holistic view of grid security. It states:[9]

> The **combination of all these technologies**, [emphasis added] **and how they are combined** [emphasis added] and implemented, determines whether the computer security personnel have effectively protected the Cyber assets.

Nor is this the only place in the FERC Staff Assessment where a more holistic view is evident but time and resources in this pro bono effort prevent citing all references. While the Utilities do not wish to discuss the **"combination of all these technologies"** as applied to the physical portion of the bulk power system, to ignore potential interactions of any type is as dangerous as taking medical drugs and/or supplements without researching dangerous side effects of their interactions (and interdependencies for the grid). "Do no harm" applies in all cases.

It is EES's opinion the aforementioned utility-"imposed" limitations on CSC prerogatives compromises any serious investigation of energy security contemplated by the General Assembly and the CSC. Additionally, in their initial comments at Point II, p. 3, second to last line, the Utilities are even presumptuous enough to add the words "may include" to the legislatively set points of investigation when the word "may" does not appear in the statute at that location but only later in reference to executive sessions. The operative statutory language is "including" not "may include". The CSC should take administrative note of this utility action to, once again, change the rules of the game by misrepresenting the legislative wording to avoid serious discussions of security matters.

II. ROLE OF THE CONNECTICUT SITING COUNCIL AND THE NERC CRITICAL INFRASTRUCTURE PROTECTION STANDARDS (CIPs)

The Utilities contend that there is no need for CSC's intent to develop Best Management Practices as this would duplicate efforts at the regional and national level and add yet another layer of regulation that may actually pose conflicts. EES disagrees. Rather than review the NERC CIPs and other standards in merely a passive role as suggested by the Utilities, this docket presents a leadership opportunity for the CSC and the parties/intervenors to actively contribute to

[7] FERC Staff Preliminary Assessment of the NERC's Proposed Mandatory Reliability Standards on Critical Infrastructure Protection. RM06-22-000. December 11, 2006.

[8] NERC Standards CIP-002 to CIP-009. Draft 1. Nov. 20, 2008. Open for public comment until January 5, 2009. Also, please note that EES has worked from redlined versions of the CIPs to better determine what has been deleted and what has been added during the most recent process opened on 11/20/08 and closed 1/5/09.

them. A history of the development of the CIPs show them to be moving target that has been through numerous versions and is still under development. The closing section of the FERC Staff Assessment places in high regard the NERC Security Guidelines for the Electricity Sector which, they note is a separate document from the CIP reliability standards. The Assessment says:[10]

> "are meant to be 'living' documents that will evolve just as the threats and challenges continue to evolve…Although NERC characterizes the Security Guidelines as "best practices," certain provisions of the guidelines address more basic security needs and may be more appropriate as Requirements… ….Throughout the preliminary assessment, staff has identified various requirements in the CIP Reliability Standard that would benefit from greater specificity. Often this greater specificity can be found in the Security Guidelines. Thus we believe that the Security Guidelines are not only an important complement to the CIP Reliability Standards, but in certain instances, provide more basic direction than the standards in developing and implementing sound security practices.[11]

Even prior to that FERC Staff Assessment a California representative to the CIP development process seems to echo what is currently being heard from local utilities:[12]

> A key strength of the proposal is that it's being driven by utilities and not by the federal government, said James Sample, manager of information security services at California Independent System Operator Corp. in Folsom. With utility-driven standards, "we can control our own destiny," Sample said.

In light of current discussions on the role of regulation (or lack thereof) in regard to collapsing financial markets and wholesale investment fraud[13], the above statement has a chilling effect. It calls into question who may be driving the process, the regulators or those being regulated, and why greater input by those with monetary interests may be driving critical security standards. It provides additional reason why the Utilities should not be allowed to change the rules of the game as set by the CSC to investigate BMPs in this docket.

No less an entity than the National Institute of Standards and Technology (NIST) has also weighed in to caste certain doubts on the emerging standards' adequacy and the need to truly standardize them and integrate Industrial Process Controls among other interdependency issues:

> 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

---

[9] At FERC page 8, paragraph 1, last three lines

[10] FERC Staff Preliminary Assessment of the NERC's Proposed Mandatory Reliability Standards on Critical Infrastructure Protection. RM06-22-000. December 11, 2006. p.40. Section XII.

[11] NOTE: A review of the NERC Security Guidelines document [Version 1, June 14, 2002] leads EES to the same conclusion on their value not just in the sphere of cyber security but in relation to physical security as well.

[12] Hoffman, Thomas. "Utility Cyberseurity Plan Questioned." Computorworld.com. May 23, 2005.

[13] The SEC was warned as early as 1999 by Harry Markopolos, then that Bernard Madoff's "financial results didn't add up". He told the SEC in 2005 that Madoff was either "front-running" or that he was "running world's largest Ponzi scheme." Wall Street Journal. January 5, 2009. Sarah N. Lynch and Siobhan Hughes.

- 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… [14]

- The management, operational, and technical controls in the NERC CIPs are a subset of the moderate baseline set of controls in SP 800-53.

  - This subset may not be adequate for protecting critical national infrastructure, especially when considering interdependencies of the critical infrastructures.

  - The moderate baseline may not be adequate for all electric energy systems when the impact of regional and national power outages is considered. [15]

There is uncertainty by EES that these concerns by NIST have been adequately addressed in CIPs 002-009 issued November 20, 2008 and open to comment until 1/5/09. As such, what the Utilities depict as "redundancy" offers an opportunity to review cited inadequacies and insure the regulatory balance lies with the regulators; not those being regulated for at least this state.

III. EES SUGGESTS A MORE COLLABORATIVE PROCESS

What EES suggests going forward in this docket includes:

EES does not believe that a topic of such tantamount importance and complexity can be adequately addressed by one CSC hearing followed by a decision. EES, with CSC approval, will acquiesce to Attorney Golden's suggestion at the 12/17/08 Pre-Hearing Conference to produce a "White Paper" on existing and proposed federal security standards promulgated by FERC/NERC/NPCC/NIST and others . The investigation leading to a White Paper might entail:

- Working collaboratively under the auspices of CSC which would convene a task force to examine what have been identified as some of the more controversial aspects of the standards as well as new considerations consideration/reconsideration.(See Appendix A for specifics.)
- Fully explore a broader view of these security standards within the context of the CSC's proposed Best Management Practices but in a holistic manner as described previously in relation to "siting" within the EES testimony. Particular focus might be on NERC's "Security Guidelines for the Electricity Sector"[16] highly touted by FERC's Staff Assessment of December 11, 2006, at p. 40.
- Not apply the findings of said White Paper as a separate Connecticut standard but provide them at the next available opportunity as input into revisions of the existing national standards which, to EES's knowledge, no State of Connecticut entity has been a party.[17]

[14] Stuart W. Katzke, Ph.D. and Keith Stouffer. Comments on the FERC Staff Preliminary Assessment of the NERC Proposed Mandatory Reliability Standards on Critical Infrastructure Protection issued December 11, 2006 Docket RM06-22-000 February 6, 2007. p. 2.
[15] Op cit p.4
[16] Version 1.0, June 14, 2002.
[17] If CSC results can be readied in time there is the "Commission on Cyber Security for the 44th Presidency, which soon will publish sweeping recommendations including the need for a comprehensive National Strategy to Secure

IV. CLOSING STATEMENT

EES believes the first responsibility of government is to the security of its citizens. Conflict that can compromise that security has changed its nature, aims and targets over time from being purely for territorial gain and wealth to ideological struggles where winning "hearts and minds" is tantamount to "victory". Today, "victory" may take on yet another face where an adversary's economy may be the most attractive target. The criticality of the economy was also foremost in an early definition of Information Warfare (IW) (of which cyberwar is one subset):

> Most clearly, though, the distinctive feature of pure IW is that it can be so easily waged against a civilian infrastructure in contrast to a military one. This is a new facet of war, where the target may well be the economic national security of an adversary. In addition, though, we have distributed the capability to wage war.[18]

As the nature of conflict constantly changes, all parties involved in this docket must also change to meet newly emerging threats; not narrow scopes of investigation. What has not changed is that, "All that is necessary for the forces of evil to win in the world is that enough good men [and women] do nothing."[19] Inaction and complacency are not options.

Cyberspace" as reported by Harry D. Raduege, Jr. in Sci-Tech Today.com on December 31, 2008 7:34AM. Also, such a White Paper may not enjoy unanimity and a minority report ought to be allowed.

[18] Winn Schwartau, *Information Warfare, Electronic Civil Defense*, Thunders Mouth Press, NY, 1996. p. 584.

[19] Attributed to Edmund Burke by Dr. Albert E. Burke, former Director of Graduate Studies in Conservation at Yale University, in Enough Good Men: A Way of Thinking. World Publishing Company (Cleveland). 1962. Flyleaf.

Appendix A

Areas of potential investigation for the CSC-sponsored White Paper may include but not be limited to:

1) Address energy security in a more holistic manner by providing some basic definition(s) that encompass the multiple forms which energy security may take and discuss the implications of each. Early in its testimony of November 25, 2008, EES provided the following as a starting point as no substantive definition had been provided in the legislation as a basis for the scope of the docket nor has it been forthcoming in the utility documents presented thus far. EES sees at least five distinct security threats to the electric grid. These include:

- Energy security in the form of fuel supply interruption/cost escalation[20]
- Physical security of grid components (generation, transmission, distribution, control rooms)
- Foreign dependency via disruption of globalized supply chains for critical grid components and minerals used in component manufacturing processes
- Cybersecurity threats including distributed denial of service, hacking, electromagnetic pulse, embedded codes in foreign sourced components
- A combined or "blended" combination of the aforementioned threats

2) Consideration/Reconsideration of some of the more controversial aspects of the NERC CIPs including but not limited to definitions of and need for [or not] the following terms and concepts:

Risk-based Assessment.

Reasonable Business Judgement.

Technical Feasibility

No standardized document retention times and no timely reviews of records, logs and more timely reporting to Electricity Sector Information Sharing and Analysis Center of incidents

Lack of even minimal standardization for Bulk Power System assets management

Role of Self Certification/Self reporting versus audits by higher authorities

Lack of specific, prescribed and meaningful sanctions/penalties as specified in the earlier Urgent Action (UA) 1200 Standard[21] (pages 22-23) but not part of CIPs 002-009 as a deterrent to errant behavior

Efficacy of paper drills versus live exercises and post "lessons learned" reviews

[20] It should be noted there are too many misconceptions which often equate energy security primarily with oil dependence. While this may be true of the economy as a whole, in the New England electricity sector with 3.3% [Corrected figure. Given in testimony at 4%] this is not a direct factor but still requires some discussion.
[21] Urgent Action (UA) Standard 1200-Cyber Security. Adopted by NERC Board of Trustees August 13, 2003.