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**

June 22, 2009
Comments
Energy Security Risks & Considerations

JOEL N. GORDES
DBA ENVIRONMENTAL ENERGY SOLUTIONS (EES)

EES appreciates the opportunity to participate in Docket #346 and offers these comments pertaining to the Connecticut Siting Council (CSC) White Paper of May 28, 2009.

I. Statutory Charge and Questions of Scope

Public Act 07-242, An Act Concerning Electricity and Energy Efficiency, Section 8, directs the CSC "**…** to investigate energy security with regard to the siting of electric generating facilities and transmission facilities, including consideration of planning, preparedness, response and recovery capabilities." It is also noted that in 2003 the Legislature added "to promote energy security" in addition to the CSC's usual environmental responsibilities.

CSC has prepared a White Paper (WP) open for testimony or comment later to become the subject of a hearing. In reviewing said WP as well as statutes and regulations governing CSC, EES was able to find information on applications, certification, filing requirements and procedures including definitions in CGS at 16-50i and in CSC Regulations at 16-50j-2a. Within the definitions of both documents, however, there was no concise definition of the word "siting" and precisely what that might entail. While it may be that a plain language interpretation is presupposed, to not have a set definition still opens the term up to a numerous interpretations. For instance the regulations at (g) say: "'Facility' means 1. An electric transmission line of a design capacity of 69 kilovolts

or more, including **associated equipment** [emphasis added]". Earlier, however, in (a) "'**Associated Equipment**' [emphasis added] means any building, structure, antenna, satellite dish, or technological equipment, including equipment intended for sending or receiving signals to or from satellites, that is an integral part of the operation of a community antenna television tower or telecommunications tower." This latter definition seems heavily related to telecommunications equipment rather than power systems but when the definitions are taken together imply that when "siting" takes place, there is a need to take into account not only the proposed facility but "associated equipment" as well. This can be supposed to extend, if distance is not specified, to include the effects on the electric grid itself. Lacking further direction in this matter, EES concludes this can refer not merely to the security of a single facility but its effect on security of the grid as a whole since the grid is comprised of many forms of associated technological equipment.[1]

It is also a fact that all electric facilities have some degree of Supervisory Control and Data Acquisition (SCADA) systems embedded in their physical structure. SCADA can also provide pathways for intrusion via several means of cyber attack. In March 2007 a video was released showing how a physical attack was accomplished to destroy a generator via cyber means through a SCADA system. One description reads:[2]

> In a dramatic video-taped demonstration of the Aurora vulnerability recorded in 2006, engineers at Idaho National Labs showed how the weakness could be exploited to cause any spinning machine connected to the power grid -- such as a generator, pump or turbine -- to self-destruct. In many cases, the researchers found, the attack could be carried out via the Internet.

While EES, in its motion of June 15, 2009, requested guidance on the issue of whether "physical" as used in the WP also included cyber, no response had been received in time for preparation of this commentary. For this reason, contrary to Utility desires, the NERC CIPs are cited both for specific purposes as well more generally where CSC could directly work with federal authorities to enhance security.

II. A Role for State Government

The argument has been made that grid security is more appropriately a federal or regional issue. In this case, however, the CSC has a direct mandate from the legislature to

[1] EES was hoping to find further direction on the term "security" in the definitions since the limitations in the WP did prompt a motion from EES for CSC to reconsider certain limitations and terms that has not been responded to by the time of this writing.

[2] Brian Krebs . *TVA Power Plants Vulnerable to Cyber Attacks, GAO Finds Regulators Want Authority to Require Security Upgrades Industry-wide*. Washington Post. May 21, 2008.

not only investigate energy security as it applies to siting in Sec. 8 of PA 07-242 but also previously in PA 03-140 (16-50g), AAC Long-term Planning for Energy Facilities, "to promote energy security." The implementation of this latter point was not expounded upon but it is proceeded by language listing the purposes of this chapter which includes: "and technically sufficient to assure the welfare and protection of the people of the state;". Additionally, conflict has changed its nature, aims and targets over time from being purely for territorial gain or wealth to ideological struggles "victory" may make the adversary's economy the most attractive target. The criticality of the economy was also foremost in an actual definition of Information Warfare (IW) provided in one early work:

> 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.[3]

Under these ground rules, there are few better ways to cripple the US than to inflict unacceptable damage onto one major driver of its economy. The US electric sector is the prime target[4]. Much of the siting and regulation of these facilities is done at the state level making this docket a legitimate venue for state security considerations.

Richard Clarke who was the Director of Cyber Security for the Department of Homeland Security also articulated it well when he said:

> "The owners and operators of electric power grids, banks and railroads; they're the ones who have to defend our infrastructure. The government doesn't own it, the government doesn't operate it, the government can't defend it. .....the military can't save us."[5]

Finally on this point, the government, through regulatory agencies[6] can, in their siting decisions enhance or deter the prospects for terrorists attacks on certain elements of critical energy infrastructure. The prestigious Center for Strategic and International Studies (CSIS) echoes Clarke's sentiment when they say:

> At the same time, the United States Armed Forces cannot defend the nation against such attacks. Lines of defense and accountability often lie in the hands of individuals and smaller

[3] Schwartau, Winn. *Information Warfare, Electronic Civil Defense*, Thunders Mouth Press, NY, 1996. p. 584.
[4] See NYT article at chttp://www.box.net/shared/2h5b7zy9g5 citing this at an ISO-NE Conference in 2002
[5] Interview of Richard Clarke by Steve Croft. "60 Minutes," segment on "Cyber War." 4/9/2000.
[6] Often with very different if not conflicting agendas.

> organizations…Yet such threats are poorly understood by those responsible for their prevention.[7]

While 9/11 was supposed to have "changed the way we think" in regards to many aspects of our lives, it appears this may not have fully translated into the way we think about critical electric grid infrastructure. Clarke's and CSIS's statements imply that the responsibility for a secure infrastructure is a shared responsibility at many levels of business …and government. While government may not be able to militarily protect it, government can take steps to lessen the vulnerabilities in the regulatory decisions it makes on a daily basis. This includes to site or not site certain facilities, how it sites them, what type of SCADA system it might have intrinsic to it, what fuel requirements or restrictions it sets for them in the siting process and whether new transmission represents a helpful redundancy or merely creates additional points of failure.

The Siting Council has certain skills, mostly in the field of environmental preservation, that may be largely applicable to planning, preparedness and actual site selection of generation and transmission systems to enhance security. Some of these basic skills are embodied in environmental principles that, by example, include:

- Diversity being an environmental consideration that can apply equally to environmental species as well as for fuel source and generation selection;

- Ecologist's Barry Commoner's "First Rule of Ecology" that "Everything is connected to everything else"[8] could be speaking of the grid as easily as it is speaking of natural cycles seeking balance within ecological oscillations and how these connections may enhance or detract from security under differing conditions; and

- The environmental parable titled "The Tragedy of the Commons" which comes from a 1968 article in Science by Garrett Hardin explains a social phenomenon characteristic of human activity wherein individuals take care of what personally belongs to them; but destroy shared resources in their haste to get what they can.[9] This, too, may have grid applicability.

Another potential role for the CSC would be to strengthen those areas where under the current federal system, there are some major weaknesses. These may include:

[7] de Borchgrave, Ledgerwood et al. "Cyberthreats and Information Security: A Report of the CSIS Homeland Defense Project." Center for Strategic and International Studies. May 2001. p. 7.

[8] Commoner, Barry. *The Closing Circle*. (Bantam Books. New York) p. 29. 1972.

[9] Op cit Commoner and http://blogs.asaecenter.org/Acronym/2009/06/tragedy_of_the_commons.html , http://en.wikipedia.org/wiki/Tragedy_of_the_commons

1) **Self Certification.** In reviewing various documents pertaining to security[10] one feature becomes evident. That feature is that many if not most of the standards by FERC, NERC, NPCC and others are subject to self-certification or audit. In an earlier era this may have been acceptable but public trust of "reasonable business judgement"[11] in 2009 to undertake self-certification may no longer satisfy the public. This is due to the disintegration of such trust in regulation of the financial sector now seen as one probable cause of the current recession. Lack of external certification and/or auditing are weak points in the system in which the state might play a "supportive" role by insuring that Registered Entities prove to the Siting Council they are up to date on such submittals to federal authorities before any new siting process can commence at the state level.

Evidence of the failure of this self-reporting may be seen in an April 7th letter from Michael Assante, Vice President and Chief Security Officer of the North American Electric Reliability Corporation (NERC), to Industry Stakeholders. In this he references NERC Reliability Standard CIP-002 pertaining to asset identification as well as the response to an earlier survey wherein a significant percentage of **expected respondents supposed to have cyber critical assets (CCA) did not respond**. [Emphasis added.] He also notes that:

> We expect to see a shift in the current self-certification survey results as entities respond to the next iteration covering the period January 1 - June 30, 2009 and when the Regional Entities begin to conduct audits in July.

Whether this portends some form(s) of no-notice, on-site inspections similar to what is employed in military operational readiness inspections can only be left to speculation. The tone of Mr. Assante's letter telegraphs this issue is to be seriously where security is concerned and that he may be looking at a more holistic, whole systems approach. (at p. 2, para. 3 of NERC Letter)

Even in the case of audits, self audits are frequently permitted and when they are conducted by external authorities, "Registered Entities" are usually provided

[10] EES appreciates Mr. John R. Morisette of Northeast Utilities supplying some of these documents in his CSC submission dated February 13, 2009, to set the parties on the same page for further discussion.
[11] Comments of Northeast Utilities Service Company, dated February 12, 2007, in remarking to the FERC on the NERC CIPs 002-009 specifically requested retention of the term "reasonable business judgement" (at p.2) which they saw as essential to provide flexibility.

advance warning for periods as much as 90 days. In such cases little is known about the day-to-day compliance and readiness of the "Registered Entities" except what they undertake by their own "reasonable business judgement".

2) Penalties. When the original version of what became the NERC CIPs were issued as Urgent Action Standard 1200 in 2003, they had as a portion integral to the document of what were termed "Sanction Tables". These provided the information by which penalties for nonconformity's to the standards were given either as types of letters sent to various company officers (VP, CEO, CEO and Chairman) within the chain of command; if a letter was not strong enough, a fixed dollar amount was assessed as a one-time fine; or a dollar per MW amount.[12] This gave a clear warning and deterrent to the private sector of what was expected if the standards were not met. Since that time, with the continuing evolution of the CIPs, the penalty section of the document appears to be a separate document (Guidance for the Enforcement of CIP Standards) with different sections becoming subject to different levels of compliance at different times. Regional Audits are to commence in July 2009.

While CSC has no direct role in this, they should consider requesting of NERC that they be notified of any non-conformities of companies operating within Connecticut and advised of any penalties incurred. CSC might then be able to refuse to approve projects in Connecticut for companies who have not complied with the NERC security standard(s).

3) Perception of Utilities Seen as Driving the Process. As noted in earlier documents in this docket, a history of development of the CIP standards show them to be a moving target that have been through numerous versions and are still under development.

But the comment below concerning the CIP development process seems to echo the position of local utilities:[13]

> 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.

[12] NERC Urgent Action Standard 1200, Cyber Secuirity. August 13, 2003. Pp. 22-23.
[13] Hoffman, Thomas. "Utility Cyberseurity Plan Questioned." Computorworld.com. May 23, 2005.

In light of current discussions on the role of regulation (or lack thereof) in regard to collapsing financial markets and wholesale investment fraud[14], the above statement has a chilling effect. It calls into question who may be driving the processes, the regulators or those being regulated, and why greater input by those with monetary interests may be driving critical security standards. A more recent account echoes this concern:[15]

> Another problem is that utilities are essentially responsible for policing themselves, said security consultant Tony Flick, who plans to offer a separate turbo talk at Black Hat [hackers' convention]. He likens the regulatory arrangement to that in the frequently criticized credit card industry, in which merchants are required only to comply with rules set by other companies in the industry. "It's kind of like history repeating itself," he said. "They're being relied upon to actually implement the standards without any oversight."

As such, one important role of the CSC is to firmly regulate those who propose projects for whatever reason and ensure they comply with federal regulations concerning security before a project can be sited.

III. Toward a More Holistic View of "Security"

In further support of taking a broader view of how CSC might want to look at security, EES reiterates its position on the word "siting" in light of events of 9/11/01 and new legislative mandates such as PA 03-140, that may require some reexamination of energy security. One insight into how we might approach "siting" comes from the National Research Council (National Academies of Science, Engineering, etc.) They have stated in regard 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).[16]

[14] 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.

[15] Dan Goodwin. Buggy 'Smart Meter" Open Door to Power-Grid Botnet". The Register. June 12, 2009.

[16] *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.

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 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 made repeatedly in earlier documents:

> … 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. [17]

EES has made it clear from its first document in this rather wayward proceeding that it does not agree with the Utilities' overly-focused approach that appears to look just at each component but not potential interactions in a more holistic approach. The dialogue within the FERC Staff Preliminary Assessment[18] of the NERC then-proposed Critical Infrastructure Protection (CIP) standards CIP-002 through CIP-009[19] adds credibility to the need for a more holistic view of grid security when it stated:[20]

> 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. The Utilities do not particularly 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, however, is as dangerous as taking medical drugs and/or supplements without researching dangerous side effects of their interactions (and interdependencies for the grid in this docket). "Do no harm" applies in both cases.

Industry personnel are occasionally too close to the subject to be either objective or they "don't know what they don't know" to even frame the right questions. Sometimes it takes a far more diverse group with multiple disciplines to frame the right questions or

[17] Letter of transmittal to first round of Docket #346 interrogatories. 10/31/08
[18] FERC Staff Preliminary Assessment of the NERC's Proposed Mandatory Reliability Standards on Critical Infrastructure Protection. RM06-22-000. December 11, 2006.
[19] 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.
[20] At FERC page 8, paragraph 1, last three lines

add value in unexpected ways. Professor Dennis Mileti[21] spoke of this problem in his November 1999 speech "An Assessment of Natural Disasters in the US" and reported that those involved in planning, mitigation and recovery come from narrow disciplines that often led to the wrong conclusions and can even lead to a worsening of disaster response, mitigation etc. So he convened 132 experts with a diversity of disciplines to investigate this enigma. He related that experts in narrow focus subject fields:

- Know what they know;
- Know what they do not know; BUT
- DO not know what they do not know

And for that last crucial reason he suggested tht policies, procedures and responses prior groups had developed for disasters was fundamentally flawed due to their narrowness of scope. His area of expertise in the sociological aspects of disaster planning, recovery, response and mitigation may have many similarities and applications to potential electric system security problems.

Looking at some of the standards kindly supplied by NU's Mr. Morisette on 13 February, the fairly standardized formats provide a purpose, applicability to parties, requirements, measures, compliance and violation levels. Separate standards exist for a number of different pieces of equipment, functions, protocols, etc. We know what we know on these standards, we know what we don't know on these standards but do we still "don't know what we don't know" on what might be missing. Who else needs to frame the requirements/question(s)? Do these seemingly stovepiped standards actually make us safer? Will our adversaries play by our rules even if all our documentation is in place?

An example of this not knowing what we did not know did take place on 9/11 when national security officials at the highest level fell victim to their own mindsets.[22]

> On April 8, the commission investigating the Sept. 11 attacks heard testimony from national security adviser Condoleezza Rice that the White House didn't anticipate hijacked planes being used as weapons. [23]

[21] Director Emeritus of the Natural Hazards Research Applications and Information Center at the University of Colorado in Boulder on Occasion of the 50th Anniversary of the Lamont-Doughterty Observatory. Columbia University, New York, NY. Speech available upon request by download at https://secure.logmein.com/f?1eB3oDAy1HMDTmC2pIdJTXXTZKwQRBeMM0XxgTAkmwm

[22] Steven Komarow and Tom Squitieri. "NORAD Had Drills Of Jets As Weapons." USA Today. April 18, 2004.

[23] EES notes that Tom Clancy wrote about exactly this use of aircraft as weapons in his 1994 book *Debt of Honor* where a plane destroyed the US Capitol with most high ranking elected officials present.

> On April 12, a watchdog group, the Project on Government Oversight, released a copy of an e-mail written by a former NORAD official referring to the proposed exercise targeting the Pentagon. The e-mail said the simulation was not held because the Pentagon considered it "too unrealistic."
>
> President Bush said at a news conference Tuesday, "Nobody in our government, at least, and I don't think the prior government, could envision flying airplanes into buildings on such a massive scale."[24]

It was these revelations that likely prompted the Kean-Hamilton 9/11 Commission to later say, "We believe the 9/11 attacks revealed four kinds of failures: in imagination, policy, capabilities, and management."[24]

EES, having never been accused of having a failure of imagination, would then pose as questions: 1) Whether "siting" (which is a prerequisite to building) ever greater amounts of equipment within a centralized system meet a point of diminishing return in regard to resiliency via redundancy? 2) Doesn't this also incorporate a greater number of points of failure as suggested by the National Science Council at p. 7, lines 220-225? 3) Isn't this potentially more prone to a cascading failure by its very centralized nature? 4) If so or even of just a questionable nature, shouldn't the Siting Council be looking at this in a more holistic way than desired by the Utilities? Set new requirements to avoid this potential problem? 5) Would greater decentralization of the grid lead to greater resiliency? These are basic questions that when posed earlier in this docket have gone mostly unanswered and the direction of the docket swaying from its previous direction of Best Management Practices to avoid dealing with them.

IV. The Coming Smart Grid

While earlier EES documents have proposed greater resiliency of the electric grid through use of distributed resources (including combined heat and power), decentralization and microgrids, nowhere in those previous documents has EES brought up the topic of what is termed the "Smart Grid". Many presuppose it is the same as distributed generation and/or microgrids but this is inaccurate. For a basic explanation of terms and comparison, the following attributes are offered for each:

> Distributed resources include conservation and load management with modular electric generation and/or storage located near the point of use either on the demand or supply side. DR includes fuel-diverse fossil and renewable energy generation and can either be grid-

[24] 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.

connected or operate independently. Distributed resources typically range from under a kilowatt up to 50 MW. In conjunction with traditional grid power, DR is capable of high reliability (99.9999%) and high power quality required by a digital society.[25]

Decentralization[26]

- Consist of many small units of supply & distribution with redundancy to back each other up;
- Units are geographically dispersed but close to demand centers;
- Interconnect with many units and not dependent on just a few critical links and nodes;
- Continue to operate if in isolated modes, so failures tend to be more isolated;
- Provide storage as a buffer so that failures tend to be gradual rather than abrupt;
- Short links at the distribution level;
- Employ qualities conducive to user-controllability, comprehensibility and independence.

The Smart Grid[27]

- Improved reliability, security (?) and efficiency through digital technology
- Optimization of grid operation
- Easier interconnection of distributed resources and end use smart appliances
- Control of demand response down to the consumer appliance level
- Provision for storage technology including plug-in hybrid electric vehicles and all-electric vehicles
- Real time information on electric pricing for transactive procurement of power
- Requires standards/security provisions for communications and interoperability of connected devices
- Requires overcoming barriers to adoption of Smart Grid technologies

While it is unknown to what degree the CSC will be asked to examine any aspects of the emerging Smart Grid (SG), it would be prudent to expect some activity with this suite of technologies that do incorporate aspects of distributed resources (both renewable and not). One major difference is that the Smart Grid, while similar to a microgrid, is more advanced in its transactive nature due to the heavy overlay of digital technology allowing a microgrid to "have a brain" and far better two-way communications between components right down to the residential appliance level. As such, it poses new challenges to security; less on the physical aspects but probably greater on the cyber considerations that can be used to physically incapacitate portions of the grid. While designers of the SG are sensitive to potential vulnerabilities, there is some question on the

[25] This composite definition comes from 2US DOE definitions, 2 EPRI definitions, 1 American Gas Association definition and 1 California Energy Commission definition. All available upon request.
[26] Lovins, Amory B. and Lovins, L. Hunter, Brittle Power, Energy Strategy for National Security, Brick House Publishing Co. (Andover, MA) 1982. pp. 215-218. This book was originally a study conducted for the Pentagon's Defense Civil Preparedness Agency.
[27] ISO-NE. Overview of the Smart Grid Policies, Initiatives, and Needs. February 17, 2009. pp. 2-3. Also see: http://knowledgeproblem.com/2009/03/02/smart-grid-technology-economics-and-policy-part-1-of-5/

prioritization of security in deployment of the components parts of the SG. Most proponents concentrate on the economic advantages of being able to reduce end-use customer usage in almost seamless ways that might even negate the need for many separate peaking generators and provide automatic real-time pricing. The addition of an enhanced SCADA-type system with far greater penetration, however, could present innumerable points of entry for malicious cyber activity. While planners of the SG speak of a "self-healing" system, prior to deployment on a large scale some state entities, which might include the CSC, ought to provide oversight and control of certain aspects relating to smart grid security.

V. Suggestions

EES would like to summarize a few, modest suggestions to the CSC (some of which have appeared earlier in this document) to aid it in better formulating and carrying out its mission which now appears to include energy security activities of one form or another:

- Define the word "security" within CSC regulations 16-50j-2a after clarification with the legislature on the meaning of "to promote energy security" and what aspects of security that is to include including physical damage via cyber means including electromagnetic pulse;
- Participate in state and/or federal-level security exercises (such as TOPOFF conducted in CT in April 2005 centering on New London) as an observer to gain better insights into the relationship of security to siting activities;
- Request that when a new member is named to the CSC that he or she have some experience in security matters although the current diversity of CSC is grand;
- Continue to explore and pursue the relationships between common resiliency solutions to both environmental and energy security as initially explored on page 4, lines 118-129 of this EES commentary as well.
- Upon application by any entity for construction of a new facility in Connecticut, require they demonstrate they are in compliance with all security reporting requirements to the NERC, FERC, NRC and other appropriate entities.
- As a cross-check to the above, request of NERC that CSC be notified of any non-conformities of companies operating within Connecticut and be advised of the penalties sanctioned.
- Deny approval of projects in Connecticut to companies that are in non-compliance with federal security mandates unless such projects are required to meet such mandates.
- Before elements of the Smart Grid are widely deployed, coordinate with federal and other state entities to ensure that security-related aspects are prioritized. Provide oversight and control of certain aspects relating to Smart Grid security.

- [28]EES pragmatically notes the state budget crisis forecast is about $1 billion dollars in the current fiscal year and projected to be $4-5 billion dollars in the coming fiscal years. EES suggests it is possible the Governor and legislators may consider transferring the responsibilities of CSC into the Department of Environmental Protection (DEP) as a cost-saving measure. For purposes of self preservation, one approach might be for CSC to sharply differentiate their role from the DEP by focusing greater attention on areas of energy security as it affects siting which is not duplicative of DEP's role. EES notes that in most public surveys concerns with security issues rate higher than environmental concerns.[29] See survey on top issues from Pew Research Center at: http://people-press.org/report/485/economy-top-policy-priority Adding some credibility to this suggestion is an e-mail dated May 28, 2009, from OPM/Energy to the Connecticut Energy Advisory Board's Chairman, wherein "Essential Services" not subject to cuts were defined as:

> …generally those (1) required to protect the public health, safety and welfare; (2) necessary to the continued provision of essential state services; (3) supporting programs or services required by federal law or court order; or (4) supporting the collection or recovery of taxes or other state revenue.

VI. Conclusion

EES appreciates the opportunity to have participated in this docket and the forbearance by CSC and the parties with the nature of the EES approach to "connect the dots" and provide differing opinions on energy security matters.

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 use the same checklists when developing their methods to compromise the operation of something as economically vital and attractive as the electric grid.

The previous example (at pp. 9-10 of this commentary) on the use of aircraft as weapons of destruction in describing what took place on September 11, 2001, is instructive to illustrate how terrorists did not operate by our presumed list of threats. Rather, they came up with their own scenario that was deemed "too unrealistic" (at p. 10, lines 289-290 of this commentary) to those in command at our federal level. The federal

[28] While EES feels some uneasiness in even suggesting this, it is the EES position that in order to eventually persuade the CSC of its crucial role in security, CSC must continue to exist.
[29] EES believes that security is directly related to many environmental drivers. See https://secure.logmein.com/f?6rg5O1mHCzY7p4wneqTPvcv6oW7CirwpMD5wlZSp5WJ for an EES presentation on same.

officials were, and apparently still are, presumed to be more appropriate for this security role than the CSC.

Narrowing the examination of what is "security" in this docket and how it may be implemented may not agree with what may be the most important admonishment of the Kean-Hamilton 9/11 Commission report which said that it was a failure of imagination that largely led to the situation. This also falls into another warning given in that same report on the inclination of both the FBI and the CIA to "stovepipe"[30]. This means to develop solutions to solve narrow goals (siting in this case) in a way not readily compatible with other interconnected considerations. While this has the appearance of being "logical" it is a luxury we may no longer be able to afford since some of those who would do us harm may not meet a standard of "logic" in a Western sense (think suicide bombers).

Some overlap or even redundancies of function, developed at the state level by the CSC in concert with others, may play a pivotal role at some future point in recognizing a weakness deemed "too unrealistic" at the federal level. This redundancy rather than total separation of function and/or focus would seem to be entirely in line with the closing words of the CSC White paper where it states, "…and concurs with the layers of oversight that protect it [the grid] by competent and responsive entities."

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