Interrogatories from Joel N. Gordes DBA Environmental Energy Solutions (EES)

The following general questions are directed to CL&P, UI and CMEEC:

EES-1 How does your utility (or CMEEC) define "energy security"? What are the primary security threats that need to be addressed and how are they examined in your internal siting processes?

EES-2 For what specific security-related threats are there formal plans to protect grid resources?

EES-3 How many full-time personnel work on issues related to grid security?

EES-4 What dollar amount and percentage of total budget is allotted to security-related functions?

EES-5 Are security-related personnel involved in design, upgrade and siting considerations of grid assets?

EES-6 Where do security-related functions rank compared with other priorities (e.g. cost, profit, safety) included in design and siting of resources ? Please list the top five in order.

EES-7 Does redundancy by siting new transmission resources add reliability? Security? Always? If not, where does it reach a diminishing return or negatively impact reliability? Security? Why might it reach such a point?

EES-8 Does redundancy in transmission in any way weaken reliability or security? If so, in what way(s)?

EES-9 What new technological enhancements have been made in the last five years that improve grid operation and that would also improve security? How have they accomplished this end result?

EES-10 What future enhancements are planned in the next two years that would further improve security? Next five years?

EES-11 Is there regulatory pressure to deny or delay the use of new technology that might enhance grid operations as well as add reliability and security due to potential electricity rate impacts?

EES-12 What elements do you believe define decentralization of the grid?

EES-13 Do you believe decentralization offers any additional security advantages compared to the currently configured grid design as sited? If not, why not? If so, why? If so, have you considered strategies to further decentralize the grid?

EES-14 Do you believe if utilities were offered a higher rate of return for decentralization efforts (including ratebasing of small generation up to 25 MW or other security-related grid upgrades) under decoupling/PBR, might this result in greater efforts in that direction? (Think in terms of utility incentives such as the program management fee of 1% to 5% (after taxes) first provided for under PA 88-57.)

EES-15 Do you see autorecloser and sectionalizer technology as a step toward decentralization? How widely deployed are these technologies at this time?

EES-16 What major grid components are primarily foreign sourced? Towers, cables, circuit breakers, reclosers, SCADA, other? Does this present challenges in timely procurement of components in a "just in time" global distribution system? Does this have security implications? What might those implications be?

EES-17 If normal communication channels used by your SCADA system were disrupted, could your portion of the grid continue to operate? Is there any backup SCADA and/or communication system capable of maintaining normal or near normal operation? Has this been tested and are written after action reports available?

EES-18 If the ISO-NE and its satellite facilities (e.g. Convex at 3333 Berlin Turnpike et al) became inoperative, what would the effect be on providing power to Connecticut ratepayers?

EES-19 Do you believe the security of the nation is linked to a strong economy which in this day and age is dependent upon reliable and secure sources of electricity?

Cyber-related questions to CL&P, UI and CMEEC:

EES-20 Does your utility believe that cyberthreats present a viable danger to grid operation? If not, why not? If so why and how?

EES-21 Does your security staff include a full time person or persons dedicated to cyber-related threats?

EES-22 How do you rate cyber threats compared to other security considerations? What is your criteria for rating relative importance of threats?

EES-23 Are you compliant with appropriate and most current NERC cybersecurity standards? Have you had any discrepancies in compliance in the past year? If so, what were the nature of those noncompliance items?

EES-24 Does your utility employ a SCADA system that might be termed a "legacy" (older, but proprietary) system or is it a Microsoft Windows-based system? A hybrid?

EES-25 What is (are) the country(s) of origin (not merely nameplate brand) of the SCADA system(s) and its components in use by your utility?

EES-26 Do you know where SCADA coding has taken place? Is it an issue of concern? If yes, what steps have been taken to examine this? Any resultant abnormalities?

EES-27 Does your utility provide training to grid operators/control room personnel in learning if and when they become victims of a cyber attack? Does this include recognizing when a loss of "situational awareness"[1] might occur? Does your utility have a simulator capable of duplicating such conditions as might be found during a cyber attack? If not, is there a cost-shared, regional facility that can be used?

EES-28 What was the effect on your system during the Blaster Worm episode in early August 2003? Was your utility IT system infected? Which portions? Did this have any effect on grid operations? Other operations? Did it affect security in any manner?

EES-29 Have you experienced additional cyber intrusions from direct hacking into your system? From viruses, worms, Trojan Horses, Distributed Denial of Service Attacks, other? How many "episodes" of suspected intrusions occur per month? per year?

For Connecticut Municipal Electric Energy Cooperative (CMEEC):

EES-30 Because you still own or are responsible for directly procuring generation for your members, do you consider fuel availability as a potential security issue?

EES-31 Do you anticipate greater use of LNG to fuel plants? Do you anticipate any security problems with this fuel?

EES-32 Do you receive power from any of the so-called "Sooty-Six" plants? If so, do you anticipate any retirements of those plants within the next 5 years? If so, have you made arrangements to acquire new resources to replace them? If so, can you offer any general details as to size, type, fuels, etc? Would it be more decentalized?

EES-33 Even if you do not lose any "Sooty Six" resources per EES-32 above, do you have any plans to site generation that is more decentralized? More fuel diverse? If yes, please elaborate.

EES-34 Do you have the capability in any large scale blackout such as the August 14, 2003 episode, to isolate operations from the rest of the grid? All towns? Some towns?

EES-35 Do you have any plans or anticipate [further] decentralizing your operations beyond maintaining your own generation and grid resources?

[1] This term, common in aerial combat, had been adopted in the *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations* where, at p. 18, it is stated "Group 2: Inadequate situational awareness at FirstEnergy. FE did not recognize or understand the deteriorating condition of its system."

EES-36 Do you have spare or arrangements to procure/share spare generation step up (GSU) transformers that may not be readably available as part of a BMP Recovery strategy in the event of a loss of one or more of these units?

EES-37 If not, from where might spares be procured? How long might it take to procure them?

EES-38 Are there any transportation problems associated with transporting them on site?

EES-39 Would absence of access to such GSU transformers compromise the operation of your system? How? For how long? Might this entail economic loss? Who would be liable for such loss(es)?

The following questions are directed to the CT Energy Advisory Board (CEAB):

EES-40 The CEAB, through the exercise of it's preferential criteria, considers reliability and diversity of fuel as two considerations.[2] Would you consider that these are elements of what we might generally term "energy security" considerations? What other elements or threats do you venture comprise the term "energy security"?

EES-41 In its preferential criteria, how does the CEAB rank reliability and diversity of fuel compared to other criteria (e.g. cost, rate impact, etc.) ? Does it carry more, equal or less weight? If less, why?

EES-42 In reviewing a resource, on a case-by-case basis, are its effects on the overall reliability and resilience of the grid as a whole considered in the assessment?

EES-43 Are there other security-related criteria that you envision being added to the preferential criteria for use in assessing reactive RFPs? If yes, what might these be?

EES-44 Does CEAB consider energy security in other deliberations under its multifaceted responsibilities (e.g. IRP)? If so how does it define the term "energy security" specifically for that purpose and what specific types of security-related threats is that term meant to convey aside from dependence on foreign oil sources?

EES-45 What single-point governmental entity has overall authority and accountability for energy security above and beyond the siting function? If there is no single point of accountability currently, which entity should be tasked with that function? Why?

EES-46 16a-35k, The Connecticut Energy Policy Act, contains language declaring "it is the policy of the state of Connecticut" (not merely OPM-Energy usually associated with Title 16a) to consider certain security-related elements. Does the CEAB believe it is also bound by this legislation? Does the CEAB believe it applies to all governmental entities including the DPUC (Title 16), DEP, CSC, DOT, DPW?

[2] Comments of the CEAB to the CT Siting Council pertaining to Docket #346, Sec. 54. October 31, 2007.