Round 2. Interrogatories from Joel N. Gordes
DBA Environmental Energy Solutions (EES)

The following general questions are directed to CL&P and UI ("the Companies"):

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

In its opposition to the need for BMPs, the Companies' joint comments cite plain meaning interpretations of statutes and state in their response that security threats "…does not relate to the siting of facilities and is beyond the scope of this proceeding."

The interrogatory then becomes: How do the Companies define the word "siting" and what elements are considered? Does this coincide with the definitions accepted by the CSC and considerations enumerated in 16-50g which contains the phrase "to promote energy security" that come from PA 03-140?

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

In their reply, the Companies maintain that "grid security" is synonymous with grid reliability. "Plain meaning" definitions from a popular dictionary provides the following which seems to provide somewhat different meanings to these terms:[1]

Reliability: "is applied to a person or thing that can be counted upon to do what is expected or required."

Security: 3. "A protection or defense against attack, interference, espionage, etc."

The interrogatory then becomes: How many full-time personnel are involved strictly in grid security as opposed to grid reliability? How many share duties pertaining to both?

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

The Companies Response is: This question does not relate to the siting of facilities and is beyond the scope of this proceeding. However, CL&P allocates an adequate percentage of its budget to security-related functions to meet industry requirements. A specific dollar amount would be difficult to estimate.

The interrogatory then becomes: The Office of Consumer Council, which protects ratepayers by examining expenditures for prudency, might find this answer ambiguous at best. Please elaborate and detail within which budget line item this would appear and the estimated amount. In addition, what is considered "adequate"?

---

[1] Webster's New World College Dictionary. Third Edition. MacMillan USA. 1997, pp. 1133, 1214.

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.

The Companies respond that: When designing and siting resources there are many factors that must be considered, including security-related functions. All of these factors must be taken into account and be given due regard with respect to each specific project

The interrogatory then becomes: Do security-related functions outrank cost and profit in the design and siting of resources? In what instances might this not occur for a specific project?

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?

The Companies respond that: Yes. Yes. Yes. Adding transmission to a power system inherently makes the power system more robust and reliable.

The interrogatory then becomes: Why does this terse response appear to conflict with the prestigious National Research Council's appraisal below? Please cite a credible third party source to verify the position taken by the Companies.

> 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).[2]

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

The Companies respond that: Redundancy in transmission increases reliability of the power system. CL&P designs transmission to meet all applicable FERC, NERC, NPCC and ISO-NE standards with regards to reliability and security.

The interrogatory then becomes: Why does this terse response appear to conflict with the prestigious National Research Council's appraisal below? Please cite a credible third party source to verify the position taken by the Companies.

> 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

[2] *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.

increases. Modeling techniques are only now emerging for the analysis of such hidden failures." (see, for example, Wang and Thorp, 2001).[3]

In addition, who physically inspects to insure the utilities comply with all applicable FERC, NERC, NPCC and ISO-NE standards? Do the responsible agencies inspect. Are these noticed or no-notice inspections? Are these self-reported inspections?

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?

The Companies respond that: Because of the highly sensitive nature of the information requested, CL&P cannot answer this question without suitable protections in place so that the information provided will remain secure, however initial implementation of the NERC CIP standards has improved security. System security has also improved via NERC standards, NPCC criteria, and ISO-NE operating procedures which continue to evolve and strengthen the grid.

The interrogatory then becomes: Repeatedly providing indiscriminant use of "security" as an excuse without careful consideration of where a more appropriate and thoughtful answer might act as a deterrent[4] provides perverse results and represents a lost opportunity to actually enhance security. This question offer an example of that since an adversary would be less likely to prey upon a system that has "advertised" its security improvements than one that has remained silent.[5] What new technological enhancements have been made in the last five years that improve grid security that might deter a prospective aggressor?

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

The Companies Respond that: Because of the highly sensitive nature of the information requested, CL&P cannot answer this question without suitable protections in place so that the information provided will remain secure, however full implementation of the NERC CIP standards will further improve security in the next two years and beyond. System

---

[3] *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.

[4] Deterrence involves three conditions and assumes the adversary to be rational in a Western cultural sense: 1) you must have the capability to inflict unacceptable losses on the enemy; 2) the enemy must know you have this capability; and 3) you must have the will to use it. Approximate definition from USAF Manual 1-1, Basic Doctrine. Circa 1964.

[5] An example of this was the broad dissemination of information that terrorist chatter indicated a possible attack on the New York Subway/transit systems possibly at Penn Station and the police bolstered their forces at key locations. See "Terror Threat Emerges on Busy Travel Day". *The Hartford Courant*, 11/27/08. P. A15.

security will be improved via NERC standards, NPCC criteria, and ISO-NE operating procedures which continue to evolve and strengthen the grid.

EES agrees with the Companies on the response to this interrogatory since revealing contemplated security enhancements telegraphs their current vulnerabilities.

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

The Companies respond that: This question does not relate to siting of facilities and is beyond the scope of this proceeding

The interrogatory then becomes: While the Companies offer their opinion unsupported by facts, pending an interim decision by the CSC on the scope of this docket, EES resubmits its original interrogatory.

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?

The Companies respond that: This question does not relate to siting of facilities and is beyond the scope of this proceeding

The interrogatory then becomes: While the Companies offer their opinion unsupported by facts, pending an interim decision by the CSC on the scope of this docket, EES resubmits its original interrogatory.

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.)

The Companies respond that: This question does not relate to siting of facilities and is beyond the scope of this proceeding

The interrogatory then becomes: While the Companies offer their opinion unsupported by facts, pending an interim decision by the CSC on the scope of this docket, EES resubmits its original interrogatory.

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

The Companies respond that: This question does not relate to siting of facilities and is beyond the scope of this proceeding

The interrogatory then becomes: While the Companies offer their opinion unsupported by facts, pending an interim decision by the CSC on the scope of this docket, EES resubmits its original interrogatory.

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?

The companies respond that: [Note: Company response mislabeled as ES-017] This question does not relate to siting of facilities and is beyond the scope of this proceeding, however grid components come from a variety of sources, including foreign. NU maintains adequate supplies of spare equipment, and also pools inventory with other utilities, to address needs including security issues.

The interrogatory then becomes: While the Companies offer their opinion unsupported by facts, pending an interim decision by the CSC on the scope of this docket, EES would like to know which grid components are foreign sourced.

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?

The Companies respond that: This question does not relate to siting of facilities and is beyond the scope of this proceeding. CL&P follows good utility practice regarding the design, maintenance, and monitoring of its SCADA Systems. CL&P has redundancy built into it SCADA system design and this functionality is tested

The interrogatory then becomes: Is the redundancy noted in the answer totally separate from the primary system?

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?

The Companies respond that: This question does not relate to siting of facilities and is beyond the scope of this proceeding, however there would be no effect, both ISO-NE and CONVEX are in full compliance with NERC Standards.

The interrogatory then becomes: The current response to a NERC standard is not a complete enough answer. If ISO and all four satellite facilities were inoperative how could power be dispatched?

Cyber-related questions to CL&P and UI:

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

The Companies respond that: This question does not relate to siting of facilities and is beyond the scope of this proceeding

The interrogatory then becomes: While the Companies offer their opinion unsupported by facts, pending an interim decision by the CSC on the scope of this docket, EES resubmits its original interrogatory.

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?

The Companies respond that: This question does not relate to siting of facilities and is beyond the scope of this proceeding, however CL&P's SCADA technology is upgraded as the technology changes.

The interrogatory then becomes: Is the SCADA upgraded to a Windows-based system? Are portions of the legacy systems also left in place?

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?

The Companies respond that: This question does not relate to siting of facilities and is beyond the scope of this proceeding

The interrogatory then becomes: While the Companies offer their opinion unsupported by facts, pending an interim decision by the CSC on the scope of this docket, EES resubmits its original interrogatory.

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"[6] 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?

The Companies respond that: This question does not relate to siting of facilities and is beyond the scope of this proceeding. In addition because of the highly sensitive nature of the information requested, CL&P cannot answer this question without suitable protections in place so that the information provided will remain secure.

[6] 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 Comment. Depending upon whether operator training does include problem recognition and maintaining situational awareness, failure to answer this question may represent another lost opportunity for deterrence and EES suggest the Companies reconsider their answer if, indeed, they do provide such training.

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?

The Companies respond that: This question does not relate to siting of facilities and is beyond the scope of this proceeding. In addition because of the highly sensitive nature of the information requested, CL&P cannot answer this question without suitable protections in place so that the information provided will remain secure.

The interrogatory then becomes: At least one system was infected by what EES suspects was the Blaster Worm. EES was on-site at NU HQ on one day of that cyber episode and observed signs posted on doors warning those returning from vacation of the event and to exercise caution. This inadvertently advertised their vulnerability and possibly further compromised their security. Please answer the original interrogatory.

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?

The Companies respond that: This question does not relate to siting of facilities and is beyond the scope of this proceeding. In addition because of the highly sensitive nature of the information requested, CL&P cannot answer this question without suitable protections in place so that the information provided will remain secure.

The interrogatory then becomes: This presents an interesting situation in that one can assume an adversary knows they have hacked into a CL&P system and probably knows what has been compromised. The Company, however, seems reluctant to allow the CSC to learn this same information that the aggressors already know. This is perverse. Please answer the original interrogatory.

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.[7] 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"?

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

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?

The following questions are directed to the Department of Emergency Management and Homeland Security (DEMHS).

EES-47 Does DEMHS have full time personnel knowledgeable in electric utility operations and security of the electric grid?

EES-48 Does DEMHS have energy emergency plans to cope with loss of power for an extended period that insures the safety of the public? two weeks or longer? In winter?

EES-49 Has DEMHS conducted exercises to cope with ice storms such as in CT in 1973 or the January 5-9^{th,} 1998 ice storm in Canada/northern New England &NY that incapacitated the electric grid over a broad area for extended lengths of time?

EES-50 Does DEHMS's own facilities have on-site, electric power back-up? Types? Redundant? How many days of fuel? How often are they tested?

EES-51 Do the utilities have regular meetings with DEHMS to share information and coordinate operations in the event of an emergency? How often. Do each of these parties have a designated liaison to communicate with the other?

EES-52 Do the utilities and DEHMS have alternate communications methods by which they could communicate with each other via radio, satellite phone or other means than normal telephone or cellular systems?

EES-53 In DEMHS testimony of November 25th, the agency suggest "looking at proposals from a global perspective." Will DEMHS please elaborate on what it means by this? Does this pertain to fuel supply dependencies, other grid component dependencies, etc. or some other meaning of "global"? Or does it mean looking at the total energy security problem in a holistic manner?

EES-54 In its testimony of November 25th DEMHS also speak of the need to consider "interdependencies". Please elaborate on what "interdependency" means in DEMHS' context and provide more detail on the issues that need to be considered.

EES-55 At least twice in the DEMHS testimony of November 25th there is mention of a need for "redundant systems". Does DEMHS also believe these redundant systems should be decentralized?[8] (see difference in the footnote below and a more thorough explanation in EES Testimony at page 18, last paragraph through page 19 (at http://www.box.net/shared/4mtcq4f6cj)

[8] For instance, the US Navy A-7 attack aircraft has redundant hydraulic systems with hydraulic lines but these lines run in very close proximity to each other rather than on the opposite sides of the aircraft. As such, they are NOT decentralized, so one piece of flak could disable both hydraulic systems simultaneously. They are redundant but not decentralized and thus still vulnerable.