STATE OF CONNECTICUT

CONNECTICUT SITING COUNCIL

Proceeding for the Implementation of Section 8 and Section 54 of Public Act No. 07-242 An Act Concerning Electricity and Energy Efficiency.	Siting Council Docket 346. December 11, 2008

Responses of Connecticut Municipal Electric Energy Cooperative ("CMEEC") to the Pre-hearing Interrogatories filed by Environmental Energy Solutions ("EES").

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-1 Response. CMEEC defines "energy security" as establishing and maintaining the reliability of electric power supply for and to CMEEC's customers, as broadly defined, as it may be adversely impacted by contingent events (whether resulting from human or non-human interventions) and, as more specifically defined, against interference or interventions resulting from intentional human actions directed at impairing the safety or reliability of the electric system. The "primary security threats" that need to be addressed are physical and cyber threats to electric generating facilities, transmission lines and control centers -- areas also addressed by extensive regulatory requirements of the Federal Energy Regulatory Commission ("FERC"), the North American Electric Reliability Council ("NERC"), the Independent System Operator – New England, Inc. ("ISO-NE", and the Northeast Power Coordination Council ("NPCC"), among others. CMEEC declines to respond to how security threats are addressed in our "internal siting processes" without a protective order to protect the confidential and sensitive nature of the material. CMEEC also notes that the scope of its response to this inquiry may need to be limited, in addition, by the Council's determination in response to pending requests for definition of the scope of the proceeding filed by certain of the intervenors in this proceeding.

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

EES-2 Response. CMEEC endeavors to protect the reliability of electric power supply for and to CMEEC's customers in all instances where there is a material risk of interruption in service, no matter what the source. CMEEC declines to respond to EES-2 any further without a protective order to protect the sensitive nature of the material. Any such response will also be limited to the Council's determination of the scope of the proceeding.

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

All of CMEEC staff works on issues related to "energy security" as defined in the response to EES-1..

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

EES-4 Response. CMEEC considers security-related functions to be an integral component of all budgeted and non-budgeted line items. These functions are not separately budgeted for. Therefore, CMEEC is not able to provide a dollar amount or percentage of total budget allotted to these functions.

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

EES-5 Response. Yes.

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-6 Response. CMEEC considers security-related functions to be an integral component of the design and siting of resources and as a result, a comparison ranking of priorities as suggested in the inquiry is not meaningful.

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-7 Response. Yes. Yes. While CMEEC believes that redundancy by siting new transmission resources generally adds reliability and security, it may not always add reliability and security. Where it does not add reliability and/or security, redundant transmission resources may reach a point of diminishing return when other measures are less costly and more or equally reliable and security enhancing.

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

EES-8 Response. CMEEC does not believe that redundancy in transmission weakens reliability or security.

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-9 Response. It is CMEEC's belief that many of the technological enhancements mandated by FERC, NERC, NPCC have improved grid security. CMEEC declines to respond further without the benefit of a protective order to protect the sensitive nature of the material.

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

EES-10 Response. **S**ee CMEEC's response to EES-9 re: protective order.

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-11 Response. CMEEC is not aware of any such regulatory pressure.

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

EES-12 Response. CMEEC believes that among other initiatives, developing and utilizing new energy efficiency technologies are elements that help 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-13 Response. CMEEC believes that decentralization in the manner discussed in EES-12 above offers additional security advantages to the currently configured grid design for the reason that it may alleviate reliance on traditional resources and enhance the robustness of the grid in response to particular failure modes. CMEEC has considered such strategies.

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-14 Response. There are a number of factors involved in determining appropriate incentives to effect desired changes in behavior by "utilities" broadly defined. Also, there are different governance regimes among publicly and privately owned utilities which may impact the effect of these incentives on utility decision-making. Subject to the foregoing qualifications, the incentives discussed in the interrogatory have some probability of bringing about the suggested changes in behavior..

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

EES-15 Response. Yes. They appear to be widely used.

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-16 Response. Grid components to the extent they are sourced by CMEEC derive from a variety of sources, both foreign and domestic. Challenges in equipment procurement occur when demand for the equipment is greater than current production capacity and therefore are not necessarily tied to the location of the particular source.

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-17 Response. Primary and backup communication protocols within the utilities and between other entities within the industry for operation of the grid have been established and are tested on a regular basis. How and when these systems are tested as well as reports are considered confidential information .

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-18 Response. If the ISO-NE and satellite facilities became inoperative, any effect on providing power to Connecticut ratepayers is mitigated because those entities have developed plans and operating procedures that take into consideration loss of facilities and actions necessary to maintain the reliability of the electric grid in Connecticut.

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?

EES-19 Response. Yes.

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-20 Response. Yes. CMEEC's actions including implementing standards developed by FERC, NERC and NPCC, reduce the overall probability of a cyber threat/attack.

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

EES-21 Response. CMEEC has information technology (“IT”) personnel that are dedicated to maintaining and monitoring CMEEC’s computer assets with respect to security and cyber 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-22 Response. CMEEC declines to respond to EES-22 without a protective order to protect the confidential and sensitive nature of the material. This response will also be limited by the Council’s determination regarding the scope of the proceeding.

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-23 Response. CMEEC declines to respond to EES-23 without a protective order to protect the confidential sensitive nature of the material. This response will also be limited by the Council’s determination regarding the scope of the proceeding.

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-24 Response. CMEEC declines to respond to EES-24 without a protective order to protect the confidential and sensitive nature of the material. This response will also be limited by the Council’s determination regarding the scope of the proceeding.

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-25 Response. CMEEC considers vendor information such as is being requested here to be confidential and proprietary information.

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-26 Response. Yes. It is not an issue of concern.

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-27 Response. CMEEC declines to respond to this question without a protective order in place to secure the confidential and sensitive nature of the material. This response will also be limited by the Council's determination regarding the scope of the proceeding.

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-28 Response. CMEEC declines to respond to this question without a protective order in place to secure the confidential and sensitive nature of the material. This response will also be limited by the Council's determination regarding the scope of the proceeding.

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?

EES-29 Response. CMEEC declines to respond to this question without a protective order in place to secure the confidential and sensitive nature of the material. This response will also be limited by the Council's determination regarding the scope of the proceeding

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-30 Response. Diversification of the fuel supply is a necessity for CMEEC for a variety of reasons, including security related reasons.

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

EES-31 Response. CMEEC anticipates that LNG will be a component of future supply. CMEEC does not necessarily anticipate any security problems over and above normal security concerns.

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-32 Response. The "Sooty-six" plants are centrally dispatched on a physical basis by ISO-NE and, accordingly, generate electricity which is consumed by electric load served by the regional power grid, including the loads of CMEEC acting as a load serving entity (or "LSE"). Information regarding CMEEC's bilateral contractual procurement of power is considered propriety and confidential by CMEEC.

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-33 Response. Yes, but CMEEC declines to elaborate on the grounds that this information is proprietary and confidential. This response will also be limited by the Council's determination regarding the scope of the proceeding

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-34 Response. Yes, for all the municipal electric utilities served by CMEEC through CMEEC's agreements with ISO-NE and Convex.

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

EES-35 Response. CMEEC has plans for decentralizing its operations.

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-36 Response. CMEEC declines to respond to this question without a protective order in place to secure the confidential and sensitive nature of the material. This response will also be limited by the Council's determination regarding the scope of the proceeding

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

EES-37 Response. CMEEC declines to respond to this question without a protective order in place to secure the confidential and sensitive nature of the material.

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

EES-38 Response. No.

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)

EES-39 Response. CMEEC declines to respond to this question without a protective order in place to secure the confidential and sensitive nature of the material. This response will also be limited by the Council's determination regarding the scope of the proceeding