STATE OF CONNECTICUT
CONNECTICUT SITING COUNCIL

RE: NORTHEAST UTILITIES SERVICE COMPANY APPLICATION FOR A CERTIFICATE OF ENVIRONMENTAL COMPATIBILITY AND PUBLIC NEED FOR THE CONSTRUCTION OF A 345-KV ELECTRIC TRANSMISSION AND RECONSTRUCTION OF AN EXISTING 115-KV ELECTRIC TRANSMISSION LINE BETWEEN MIDDLETOWN AND NORWALK	:	**Docket #272**

January 22, 2004

Statement of Limited Appearance

Energy Security as a Risk Consideration in New Transmission Line Projects

JOEL N. GORDES
DBA ENVIRONMENTAL ENERGY SOLUTIONS (EES)

I. IDENTIFICATION AND QUALIFICATIONS

Q: Please state your name, position and business address.

A: My name is Joel N. Gordes, President of Environmental Energy Solutions. My office is located at 97 Eno Hill Road, Winsted (Colebrook), CT 06098.

Q: Summarize your qualifications.

A: I am an independent energy consultant specializing in energy efficiency, renewable energy, climate change as it affects the insurance industry and issues pertaining to energy security matters. I have been involved in the energy field for the past 29 years in a variety of capacities involved in active and passive solar system design, technical analysis, program operations, program design, strategy development, policy development, legislation and energy association management.

In recent years my work has concentrated on consulting to the State's Energy Conservation Management Board (ECMB) as its Technical Coordinator, consultant to the Connecticut Clean Energy Fund, consultant to the Pace University School of Law Energy Project, Executive VP of the NY Solar Energy Industries Association, and several other private and public sector accounts that periodically call upon my services. A copy of my resume pertinent to this subject area is attached as Appendix A. I want to stress that, today, I am here as an individual and representing none of these groups.

II. INTRODUCTION AND SUMMARY

Q: What is the purpose of your direct testimony?

A: The purpose of my remarks is to provide information pertaining to how increasing transmission capacity using just 345 kV lines as a fix for grid transition problems may actually weaken the resilience of the grid rather than improve it due to the potential of cyberattacks against a heavily centralized system.

I come not as an expert in transmission or even cyberattacks[1] but mostly in the capacity of a "messenger" from others who are experts or have access to experts. I seek to inform the Connecticut Siting Council, other regulators and the utilities that there is a

[1] From most accounts, it appears that the nineteen 9/11 hijackers were neither experts in landing aircraft or in structural engineering of buildings but that didn't appear to alter the outcome. Pages 24-25 of this statement clearly shows that a rank amateur, with little training, can become capable of inflicting serious harm to the grid via cyber means.

growing body of evidence that explicitly indicates that continuing to build our electric grid as we have in the past will leave our more digitally-dependent society in a far more vulnerable position. The information concerning this growing vulnerability has obviously not yet entered either the public consciousness or that of utility executives or planners or their regulators at all levels of government here in Connecticut since I have not seen it discussed in relation to these projects. Failure to address this concern has the potential to inflict large economic and even life-threatening penalties that could open up litigation to those involved in the ownership, operation, planning and regulation of the electric grid. The term "connect the dots" has become fashionable in the last few years and so I quote from many sources who have observed the energy vulnerability situation from different vantage points than the regular players that come before this Siting Council.

Q: Isn't national defense a federal issue that cannot and should not be addressed at the state level?

A: Normally national defense would be handled at the federal level, however, in the case of cyberattacks Richard Clarke who was the Director of Cyber Security for the Department of Homeland Security (Gov. Ridge's organization) stated:

> "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."[2]

The prestigious Center for Strategic and International Studies (CSIS) echoes this 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

[2] Interview of Richard Clarke by Steve Croft. "60 Minutes," segment on "Cyber War." 4/9/2000.

> and smaller organizations…Yet such threats are poorly understood by those responsible for their prevention.[3]

While 9/11 was supposed to have "changed the way we all think" in regards to <u>all</u> aspects of our lives, it appears this has not been translated into the way we think about critical electric grid infrastructure that is promoted and largely approved at the state level through such bodies at the Siting Counsel, DPUC and the DEP. Richard Clarke's statement on the previous page makes it clear that the responsibility for a secure infrastructure is everybody's responsibility-- at all levels of business and government. While government may not be able to protect it, government can certainly take steps to lessen the vulnerabilities in the regulatory decisions it makes on a daily basis by not setting up what may be, in effect, a better "targets for terrorists" program.

Q. What leads you to think that those in positions of power such as Siting Council, FERC, the ISOs, the DPUC , the utilities and others are not already addressing your concerns but are reluctant to divulge it due to their own security concerns?

A. In conversations with some members of the Siting Council, the DPUC and utility executives I was unable to discern any prior familiarization with the topic of cyberterrorism/cyberwar. While some have shown some concern over physical attacks, most had not yet fathomed that the same precautions for physical attacks may not suffice to counter cyberthreats. In at least one case the suggestion of using distributed generation as an alternative to large transmission projects has been met by derision and in several instances less than candid, unbiased information has been publicly supplied to Connecticut regulators and legislators by the ISO-NE and Northeast Utilities.

---

[3] 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.

Q: What are your qualifications to speak on energy security issues?

A: My initial training was that of professional military officer and my entry into the energy field in 1975 was based largely upon energy security motivations mostly concerning overdependence on oil from foreign sources. I also expounded upon the vulnerability of the grid to natural and man-made hazards as early as 1978 when I was first specifically published on the topic in a very pointed letter to the editor. I have also read extensively on related areas and collected information from numerous sources as evidenced by the citations used. Some of my more recent works on energy security/resilience include:

Energy Security: A Driver For DG--Looking at Local Perspectives. Presentation for the American Solar Energy Society. Austin, TX. June 26, 2003.

Rating the States for Energy Security. *Paper and presentation for the American Solar Energy Society Solar 2003 conference with Susan Gouchoe and Steve Kalland of the North Carolina Solar Center of UNC. Austin, TX.June 24, 2003.*

Cyberthreats and Gird Vulnerability. Presentation for the InfoWarCon Conference. Washington, DC. September 5, 2002.

Distributed Power Generation, *Contingency Planning & Management, March/April 2001. pp 36-38.*

The Power to Insure: Reducing Insurance Claims with New Power Options, *a project under a US DOE contract with the Northeast Sustainable Energy Association. September 2000.*

PV-Powered Wireless Telecommunications Systems, Prepared for the Rhode Island Renewable Energy Collaborative and the Connecticut Clean Energy Fund. April 29, 2000.

Distributed Renewable Energy and the Environment—Domestic Drivers and Barriers. [revised June 1999 with energy security drivers] Decentralized Energy Alternatives Symposium. Sustainable Development Initiative of the Columbia Graduate School of Business. March 15, 1999.

In addition, in May of 1999 I supplied input on consideration of cyberthreats to the electric grid to the National Security Study Group (Hart-Rudman Commission) that was tasked with planning the look of the military for the 21st century. I have also given private and public presentations on the topic of distributed generation for grid security numerous times to a wide variety of groups and individuals including:

Columbia University Sustainable Development Initiative, NYC, NY March 15, 1999
CT Business & Industry Association - June 6, 2001
CT. Clean Energy Fund Biomass Conf-June 26, 2001
Environmental and Energy Study Institute-Washington DC, February 5, 2002
Connecticut Legislative Policy Working Group-February 2002
Connecticut Energy Advisory Board-March 5, 2002
Northeast Sustainable Energy Association ReNew Conference
Mar 21, 2002
Mar 22, 2002
Mar 22, 2002 Evening Forum
Commissioner L. Kelly, CT DPUC 4/29/02
Earthday NY-May 1, 2002 Power to Insure
OCC-Mary Healey 5/8/02
Department of Public Utility Control -Norwalk Town Hall 5/10/02
American Solar Energy Society (ASES) -June 18, 2002
Northeast Sustainable Energy Association-June 27, 2002
CT SWCT Transmission Study-July 18, 2002
Ozone Transport Commission-August 6, 2002
InfoWar Con2002, Washington, DC-September 4, 2002
CT Power & Energy Society-September 12, 2002
NESEA March 12 &13, 2003-Track Co-chair
Air & Waste Management Association of Connecticut March 18, 2003
Mid Atlantic Sustainability Conference- 6/5/03
ASES 6/24/03-Rating the States for Energy Security-Main Conference
ASES 6/25/03 -Energy Security:Driver for DG- Energy Security Session
ASES 6/26/03 - CyberThreats & Local Options-Solar is Safety Session
International Conference on Advanced Technology & Homeland Security-Sep. 26, 2003
InfoWarCon, Washington, DC -October 1-2, 2003
Institute for Sustainable Energy Conference, Mohegan Sun - Oct 28, 2003
New Britain Symposium-Trinity on Main, Nov 3, 2003
Association of Records Managers and Administrators-Orlando, FL-Nov 11,2003
Back-up & Crit1ical Power Conf. IQPC-Boston, MA - Nov 17-18, 2003

Q: What is cyberwar/cyberterrorism?

A: In its most generic definition it is a form of information warfare that has been defined thusly:

> I maintain that true Information Warfare [IW] is the use of information and information systems as weapons against target information and information systems. IW can attack individuals, organizations, or nation states (or spheres of influence) through a wide variety of techniques:
>
> - Confidentiality compromise
> - Integrity attacks
> - Denial of service
> - Psyops

- Dis/Misinformation, media, etc.

> 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.[4]

More specifically for our purposes, in one form, cyberwar involves the use of computer hacking (codes, viruses, worms, Trojan Horses, dis/misinformation) to incapacitate portions of the critical infrastructure from anywhere in the world. This means the potential loss of electric service, natural gas and other pipelines, communications and our transportation systems.

In another more physical form there is what is called the E-bomb that can incapacitate any appliance, generator, auto or other device that has incorporated silicon-based semiconductors or chips. This takes place when a relatively inexpensive device (~$400) called a flux compression generator is used to induce an electromagnetic pulse similar to what accompanies a nuclear blast.[5] This is a not a hi-tech device to build nor does it require a sophisticated aerial delivery system since the device could take on various shapes and be delivered via any vehicle from a light aircraft to a UPS truck. Its effective area is limited by such variables as size, altitude at detonation, distance from critical electronics and nature of shielding materials used if any. Unless the electronics in question are “hardened” against such a weapon or placed in what is termed a “Faraday” cage, they become useless and you are effectively “back to the stone age.”

Q. Are there any other threats that might impact the transmission grid?

---

[4] Winn Schwartau, *Information Warfare, Electronic Civil Defense*, Thunders Mouth Press, New York, 1996. p. 584.

[5] Wilson, J. “E- Bomb,” Popular Mechanics. 9/2001. pp. 50-53.

A. Oddly enough, distantly related to electromagnetic pulse, there is a similar natural phenomenon that can produce similar results. In late October, 2003 what is termed a "corona mass ejection" (CME) had taken place which, in this case, sent a huge amount of charged particles toward the Earth. In March of 1989 a similar such event knocked out the Quebec power grid in Canada. What was strange in the 2003 cases was that the "solar maximum" for sunspot activity which spawns these events takes place on a fairly regular 11 years cycle the last of which occurred in 1990. A CME of this magnitude would not be normally expected during 2003. Any potential for more off-cycle activity of this nature is yet another supportive reason to consider what is advocated in these remarks for a resilient system thate could mitigate damage from such an event.[6]

Q: Please summarize your testimony.

A: My testimony will: 1) establish a case that the grid is vulnerable to physical and cyber war/cyber terrorism 2) establish definitions, the state of art and availability of distributed generation as a more secure alternative to large transmission grid upgrades 3) provide a six point cyberdefense plan that might benefit the integrity of our power system as well as supply employment opportunities in Connecticut 4) provide additional questions that regulators might ask those in favor of large transmission projects 5) provide a closing statement.

Q: Please summarize your recommendations.

A: My recommendations are embodied in the six point cyberdefense plan mentioned immediately above in numeral three. They include:

---

[6] Cynthia L. Webb, *The Perfect Storm?* Washingtonpost.com. Wednesday, October 29, 2003

1) Large new transmission line plans by NU and other utilities across the nation to alleviate power congestion further centralizes energy make us more vulnerable to cyber and physical attacks. Any grid upgrades should also include provisions first to make the electric grid, like the internet, self healing and, when required, “adaptive” in order to isolate into micro-grids.

2) Use of load management and small, fuel diverse generators that are more widely dispersed provide a more robust system less vulnerable to physical and cyber attacks that should be come as primary steps before large transmission projects are instituted.

3) Because many Connecticut firms produce these distributed generators such as gas turbines, turbine components and fuel cells, this could provide a major economic boost to make up for lost aircraft engine sales and insurance losses due to 9/11 terrorism fears.

4) Under an optimalized program, distributed generators would be mostly paid for by businesses and placed on their premises (not utility property at a cost to ratepayers) to run in parallel to the grid to insure power reliability and quality. As such, the cost may be less than transmission lines for which ratepayers would subsidize the entire bill.

5) Because most are extremely clean, small or use renewable sources, distributed generation options for congestion alleviation may be quicker to implement than power lines due to less DEP and Siting Council delays and outside legal challenges.

6) Utilities should be allowed to build and ratebase diverse, demand-side, distributed projects up to 25 megawatts in size to provide them incentive not to oppose alternatives that are in the best interests of the nation. Regulators should consider enhanced rates of returns for this activity.

III. THE CASE FOR GRID VULNERABILITY IN A DIGITAL SOCIETY

Q: Why do you feel it is necessary to build a case for grid vulnerability to cyberthreats?

A: I do not believe there is a general consciousness on this issue, particularly as to how the grid could be affected by cyberthreats. I hope to establish a case that the grid is vulnerable to not only natural and man-made physical attacks but also cyberwar/terrorism and begin the germination process to integrate cyberwar/terrorism into the national, state, utility and regulatory consciousness in terms of transmission and distribution system vulnerability. Nor am I the only one to hold this view:

> There is a discussion that sometimes takes place around SCADA[7] systems… inevitably I have this discussion every week from the west coast to the east coast. Inevitably it unfolds like this: Someone says, "Well, you know that we have an isolated network..we have a complex isolated network." And they are deluding themselves in those cases because there are modems for vendors to conduct maintenance, there are modems for workers to access their AOL accounts and there are connections between their system and the internet as recent virus and worm attacks have shown. And then they say, "Well, even if they got in they wouldn't know [what] to do because our systems are secure through obscurity; they're proprietary; they're SCADA. You have to be invited and trained in the dark, mystical art of being a SCADA operator to fully understand our system." Fact of the matter is this is not true; SCADA interfaces are graphical and, as will be born out, are able to be exploited by anyone with any degree of computer literacy.[8]

Even the US-Canada Power System Task Force's (blackout) draft report, in one of its more lucid portions of Chapter 8, is in agreement with Dr. Flynt's statement:

> In electric power, SCADA includes telemetry for status and control, as well as Energy Management Systems (EMS), protective relaying, and automatic generation control. SCADA systems were developed to maximize functionality and interoperability, with little attention given to cyber security. These systems, many of which were intended to be isolated, are now, for a variety of business and operational reasons, either directly or indirectly connected to the global Internet… The existence of both internal and external links from SCADA systems to other systems introduced vulnerabilities.[9]

---

[7] SCADA refers to Supervisory Control and Data Acquisition Systems used to control and provide information on many aspects of power system operations.
[8] William Flynt, Ph.D., *Terrorism and the Electric Power Infrastructure*, Keynote Session, International Conference on Advanced Technologies for Homeland Security, UCONN, September 25, 2003.
[9] US-Canada Power System Outage Task Force: Causes of the August 14th Blackout. pp. 94 & 99.

Once consciousness of the seriousness of the threat is established it should promote changes to the entire process used in gas and electric transmission project planning to include national/energy security considerations that are largely lacking or misunderstood due to overemphasis on physical attacks which are somewhat different from cyberattacks.

Finally, these remarks will provide a written record that can be cited for future litigants who may be aggrieved by loss of power that might have been avoided by incorporating adequate energy security considerations into power planning by distribution companies, their regulators and all others responsible for recommendations to such regulators, legislators and other government officials.

Q: When was this cyber vulnerability first recognized and what are the potential repercussions for a cyberattack against a digital society such as our own?

A: One interesting incident that identifies when it was first recognized locally as well as offers great insight into the potential repercussions took place in downtown Hartford on February 20, 1983 when a crow took out power to the central part of the city. The Hartford Courant recounts:

> Travelers [Insurance] Cos. was forced to go into an emergency data- recovery exercise that had not been attempted in recent memory, explained Travelers senior Vice President Peter Libassi. It took Travelers four hours after the crow landed to get the computers under control.
>
> "Sometimes you have to wonder just how advanced technology is when something like this can cause these problems with this kind of equipment. We'll eventually be able to recover everything, but we're lucky this didn't happen on a weekday when hundreds of our field offices across the country would have had to shut down. .Potentially this could have cost the company a lot of money."[10]

That incident, was a precursor to the effects that could take place on a much larger scale today in a society that now has a PC on almost every business desk top; that was before we became so digitally dependent. To provide an idea of how large business losses could become, the chart below supplies the cost per hour of down time for various types of digital businesses:

Industry	Average Cost of Downtime	Source[11]
Cellular Communications	$41,000 per hour	Teleconnect Magazine
Telephone Ticket Sales	$72,000 per hour	Contingency Planning Research-1996
Airline Reservations	$90,000 per hour	Contingency Planning Research-1996
Credit Card Operations	$2,580,000 per hour	Contingency Planning Operations-1996
Brokerage Operations	$6,480,000 per hour	Contingency Planning Operations-1996
Grocery Store	$50-80,000 per day	http://www.eren.doe.gov/distributedpow
Electronic Chip Fabrication Plant	$62 million per episode	Electronic Buyers News[12]
Average Small Business	$7,500 per day	Impulse Research of Los Angeles-1998

Additionally, a federal judge in Arizona ruled that property insurance covering "physical damage" also covers damage from loss of computer data, access, use, and functionality. The decision stated:

> At a time when computer technology dominates our professional as well as personal lives, the Court must side with Ingram's broader definition of "physical damage." The court finds that "physical damage" is not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use and functionality. …Lawmakers around the country have determined that when a computer's data is unavailable, there is damage; when a computer's services are interrupted, there is

---

[10] Stertz, B. "Crow Short-Circuits Phone, Power," *The Hartford Courant*. 2/20/1983.

[11] The first five business losses were attributed to Kim Barnes, "Deregulation: Differentiate Your Energy Services Business by Providing Customers with Computer Grade Power and Reliability," Energy.com, 7 April 1999. The last line for average small businesses came "AlliedSignal: Power outages cost small business big bucks," PMA OnLine Breaking News, 1 February 1999. The article specifically stated, "The importance of reliable electric power can not be over emphasized for the nearly 90% of small businesses in the United States who reported experiencing at least one power outage during 1998. According to a survey of 500 small business owners sponsored by AlliedSignal Power Systems Inc., these same small businesses reported an average of three power outages last year, costing each business an approximate average of $7,500 per day."

[12] Sandy Chen, "Huge Blackout in Taiwan Affect Chip Industry," Electronic Buyer's News, 7/30/99.

> damage; and when a computer's software or network is altered, there is damage. Restricting the Policy's language to that proposed by American would be archaic.

In this case, even though electric service was restored within a half hour, because programming for three mainframe computers was lost, those computers remained unusable for considerably longer and connections between the company's data center and six other locations were not restored for eight hours.[13]

Should that decision, which failed to gain permission for appeal,[14] become widespread, business interruption claims based on lost data could skyrocket. Aside from traditional steps such as raising premiums, setting higher deductibles, and encouraging contingency planning for such outages, insurers might look to filing suit against system operators (ISOs), distribution companies and regulators for some form of negligence in not designing a more resilient grid that is better able to reduce losses.

Q: Aside from yourself, who is concerned with threats, and particularly cyberthreats, to the gird?

A: For one, the National Research Council (National Academies of Science, Engineering, etc.) has stated in regards to adding transmission lines for relief of congestion:

> 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).[15]

[13] "Insurance Coverage Ordered for Lost Computer Data, Mealey's Reports," PRNewswire, June 1, 2000.
[14] US Court of Appeals for the Ninth Circuit Denies the Insurance Company's Permission to Appeal Ingram Micro Decision (continued). AKO Policyholder Advisor. November 2000, Vlume 9, No. 11.
[15] *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.*

They are concerned that while adding more transmission capacity may alleviate one problem (congestion) it may open up new vulnerabilities by adding greater complexity. Their concerns are well-founded as lessons from other technologies indicate that merely increasing redundancy but doing so still within a centralized system may not add overall system resiliency. For example, the hydraulic controls on the A-4 Skyhawk fighter aircraft has a duel system (redundancy) but because both hydraulic lines are in close proximity in certain critical areas, there is a higher likeliness that antiaircraft ordinance can disable both systems simultaneously.[16] While it is "redundant" it is not adequately "decentralized" and still vulnerable in this analogy.

There are also a number of former and present government and military officials (some extremely high ranking) and private sector leaders who have openly expressed their concern that cyberattacks have the potential to inflict severe damage upon the nation. Many times their statements have been included as part of larger news releases and the cyber aspects may have been lost. For the record, below is a litany of the statements, the people who made them and the source of the information:

Winn Schwartau
Cyber Expert and author of Information Warfare

> Modern societies are composed of four critical, highly interrelated, and symbiotic infrastructures upon which their national and personal survival depends: The power grid is the foundation of it all. We run it all on electricity, no matter how it is generated, and distribute it over a huge web of overhead wires and underground cables...[17]

U.S. Senator John Kyl (1998)

> Well, cyberterrorism is surprisingly easy. It's hard to quantify that in words, but there have been some exercises run recently. One that's been in the media, called Eligible Receiver, demonstrated in real terms how vulnerable the transportation grid, the

[16] Discussion with John Millar, a former Naval Aviator on 8/23/03.
[17] Winn Schwartau, Information Warfare, "Electronic Civil Defense," Thunder's Mouth Press, New York, 1996. p. 43.

electricity grid, and others are to an attack by literally, hackers--people using conventional equipment, no "spook" stuff in other words.[18]

Admiral Herbert Brown, Deputy Commander
U.S. Space Command

Virtually any country that has a computer has an opportunity to enter into cyberspace and be disruptive. … [The ability to bring down a power grid] is absolutely real .

Let me give you a quick example, I drive a 1961 Corvette. I've never had a computer problem in that car. It always runs. My wife drives a new automobile that's got a computer system in it that's a big pain … That's because the computer chip …brings that wonderful automobile to a complete standstill . So why would you think that a grid that is dependent upon computers would not be like that automobile? Certainly, this is not theory, this is very real.[19]

Richard Clarke, Former Director
Office of Cyber Security
Department of Homeland Security

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. This is the first time where we have a potential foreign threat to the United States where the military can't save us. [20]

Michael Totten
World Resources Institute

Since large, centralized energy systems are repeatedly singled out in these reports as one of the most vulnerable parts of society's critical infrastructures, the implication is clear: transition to more resilient distributed power systems which, if they fail, do so gracefully, not catastrophically.[21]

Sam Nunn, Former Senator
President's Commission on Critical Infrastructure Protection

The good news is that examination of serious issues has started...The public really hasn't focused on the fragility and vulnerability of the infrastructure and there won't be much action until that happens....On a scale of 1 to 10, public awareness is probably at a 2.[22]

---

[18] James f. Dunniagan, The Next War Zone, September 2003.p. 69.
[19] Steve Croft with Admiral Herbert Brown on "60 Minutes," segment on "Cyber War." 4/9/00.
[20]op. cit. "60 Minutes"
[21] Correspondence from Michael Totten of 1/26/99. p. 12.
[22] M.J. Zuckerman, "Targeting Cyberterrorism: Government Declares War to Protect USA's Infrastructure," USA Today, 10/20/97.

President William J. Clinton

> Last May, at the Naval Academy commencement, I said terrorist and outlaw states are extending the world's fields of battle, from physical space to cyberspace…
>
> We must be ready -- ready if our adversaries try to use computers to disable power grids, banking, communications and transportation networks, police, fire and health services -- or military assets.[23]

R. James Woolsey
Former Director, CIA

> Cyberterrorism is only one of the ways in which our energy security could be threatened by terrorist actions. … Another [way to reduce vulnerability] is to move toward reliance on renewables including photovoltaics, wind and biomass to generate electricity. Fuel cell developments for both automobiles and electricity generation are also promising. Hunter and Amory Lovins wrote 20 years ago in Brittle Power about the vulnerability of our power systems for electricity and fuel--unfortunately they are still correct.[24]

Condoleezza Rice
President Bush's Nat'l. Security Advisor

> It is a paradox of our times: the very technology that makes our economy so dynamic and our military forces so dominating -- also makes us more vulnerable. ….
>
> Our gaming exercises have told us for some time now that a few well-organized hackers could disrupt everything from our power lines to our 911 systems.
>
> And everyday it is driven home to us that the threat is not just theoretical... Protecting our nation's critical infrastructure can only be done in concert with private industry.[25]

Donald Rumsfeld
U.S. Secretary of Defense

> The Pentagon's two war strategy has outlived its usefulness, leaving the United States ill-prepared for emerging threats such as ballistic missiles and cyberattack.[26]

Richard Clarke, Former Director
Office of Cyber Security
Department of Homeland Security

> We could wake one morning and find a city, or a sector of the country, or the whole country have an electric power problem... because there was a surprise attack using

[23] Office of the Press Secretary, The White House. Speech at the National Academy of Science, 1/22/99.
[24] Transcript of radio show Global Focus: Talk about Terrorism with R. James Woolsey, 5/03/99.
[25] Condoleezza Rice, Bush Nat'l. Security Advisor at a Partnership For Critical Infrastructure meeting 22 Mar 2001.
[26] Secretary of Defense Donald Rumsfeld in testimony to the House Armed Services Committee. June 21, 2001.

information warfare.

Clarke, speaking at a cyberthreat summit, said most Americans fail to realize how dependent they have become on computers - ... to run their electricity ... and other infrastructure systems. Clarke compared the reliance to former drug addicts enrolled in a recovery program.

"We need to take a lesson from that - at least they know they have a dependency problem. Many of you are still in denial. [27]

Michael Vatis, Former Director
FBI's National Infrastructure Protection Center

"We clearly need to be prepared for serious terrorist cyber attacks on critical information systems." The tools of cyber crime, according to Vatis, "are increasingly sophisticated and available to anyone who can access the Internet."[28]

David Garman
Bush Assistant Secretary of Energy

Aside from its obvious environmental benefits, solar and other distributed energy resources can enhance our energy security…It also makes our electricity infrastructure less vulnerable to terrorist attack, both by distributing the generation and diversifying the generation fuels…So if you're engaged in this effort, it is my view that you are also engaged in our national effort to fight terrorism.[29]

R. James Woolsey, Former Director of Central Intelligence
Admiral Thomas H. Moorer USN (Ret) Former Chairman, Joint Chiefs of Staff
Robert C. McFarlane, Former National Security Advisor to President Reagan

Our refineries, pipelines and electrical grid are highly vulnerable to conventional military, nuclear and terrorist attacks.

Disbursed, renewable and domestic supplies of fuels and electricity, such as energy produced naturally from wind, solar, geothermal, incremental hydro, and agricultural biomass, address those challenges. Fortunately, technologies to deliver these supplies have been advancing steadily since the Middle East fired its first warning shot over our bow in 1973. They are now ready to be brought, full force, into service.[30]

---

[27] Richard Clarke, [Currently], Director, Office of Cyber Security, Homeland Defense Council. 11/4/99.

[28] Op cit. de Borchgrave, Ledgerwood et al. p. xi.
[29] Asst. Sec of Energy David Garman, US DOE 10/02/01 at the UPEx'01 Conference in Sacramento, CA.
[30] From a letter was sent to the Senate Majority and Minority Leaders, as well as the chairmen and ranking Republican members of the Agriculture, Nutrition and Forestry; Appropriations; Armed Services; Energy and Natural Resource; Environmental and Public Works; Finance; and Foreign Relations Committees by R. James Woolsey, Former Director of Central Intelligence, Admiral Thomas H. Moorer USN (Ret) Former Chairman, Joint Chiefs of Staff and Robert C. McFarlane, Former National Security Advisor to President Reagan. September 19, 2001.

Lt. Colonel William Flynt, Former Director
Threats to Critical Infrastructure
Office of Foreign Military Studies, U.S. Army

> In a single-superpower world , there a single best target…You're the best face of that target. Your corporations [power companies] are the best target set.[31]

James Castle, Manager of Operations
ISO-NY

> "….James Castle, manager of operations at the New York Independent System Operator, or ISO, said the system was usually operated by running the cleanest and least expensive generating stations. But the system could be less vulnerable if plants close to the high demand cities were started up, to minimize the importance of transmission lines."[32]

James Fortune, Program Manager
Electric Power Research Institute (EPRI)

> We do know that surveillance has increased, from the Middle East,… Where do you think the majority of these probes have gone? To us, the overall energy system…Are they surveilling now? That's what you do before you launch an attack.[33]

> [During] 11/97 "[Operation] Eligible Receiver" simulated cyber attack using off-the-shelf hardware and software from Internet on U.S. communications and power grid as prelude to attack on S. Korea. <u>*Finds easy access to grid*</u>. [During] 10/99 "[Operation] Zenith Star" simulated attack on 911 systems and power facilities around military installations near major cities. <u>*Shows little improvement in system security*</u>. [34][Emphasis is as in the original.]

> There are very real threats to any nation's critical infrastructure. Electrical systems are tempting and likely targets to attack by a variety of individuals and/or organizations (engaged in both sabotage and industrial espionage). Intrusion tools are becoming more sophisticated and dangerous. <u>**AND WE ARE BECOMING MORE VULNERABLE THAN EVER!**</u> [35][emphasis is as it is in the original document.]

James K. Kallstrom, Director
New York State Director of Public Security

> The electricity executives got a pep talk from James K. Kallstrom, the New York State director of public security, who said that a loss of electric service would have "a dramatic major impact to every facet of our economy." But speaking of the power

---

[31] Matthew L. Wald, "Electric Power System is Called Vulnerable, and Vigilance is Sought," New York Times. 2/28/02
[32] Op cit., Wald.
[33] Op cit., Wald
[34] Cyber Threats and Vulnerabilities to the Electric Power Industry. James Fortune, Electric Power Research Institute. February 27, 2002. Powerpoint slide # 7.
[35] Op cit., James Fortune, slide # 9.

plants and transmission lines, he added, "we have not build these things with the condition we have today in mind."[36]

Q: Are there any historical precedents of which you are aware that are similar in nature where a perceived but ignored threat came to pass? What were the circumstances and the results?

A: Yes, Pearl Harbor could be said to be a very similar historical precedent and, coincidentally, the cyberthreats I am alluding to have been called a “digital (or electronic) Pearl Harbor” waiting to happen.

Few Americans realize that there were specific warnings that Pearl Harbor would be attacked. Like Pearl Harbor, there is no reason to suppose a digital attack should be a surprise to those who have recognized the changing nature of threat, educated themselves on those threats and processed the available information to come to this conclusion. Unfortunately, many of those involved in grid upgrade are apparently unaware of this information or, if they are privy to it, appear to have processed that same information differently or for some reason may have just chosen to ignore it. They may have chosen not to heed these warnings signs or it may be that the utilities and some of their regulators are merely taking a “technician’s” view to their approach on transmission planning (sometimes due to the way in which the enabling legislation is written for regulators). Sir Richard Livingston once defined a technician as “a man who understands everything about his job except its ultimate purpose and place in the order of the universe.”[37] In a post-9/11 world we can’t afford to continue to be “technicians” or employ those who are.

In the case of Pearl Harbor, as early as 1924 and again in 1926 Brigadier General Billy Mitchell warned that:

---

[36] Op cit., Wald.
[37] Vogt, William. Road to Survival. (William Sloane Assoc.) New York, NY. Copyright 1948. p. 272.

> "…I am convinced that the growing airpower of Japan will be the decisive element in the mastery of the Pacific…Air operations for the destruction of Pearl Harbor will be undertaken…The attack to be made on Ford Island at 7:30 a.m… The Philippines would be attacked in a similar manner…The initial successes would probably be with the Japanese. [1924]
>
> A surprise aerial attack on Pearl Harbor will take place while Japanese negotiators talk peace with the U.S. officials, moreover the attack will come on a Sunday morning. [1926][28A]

Information Warfare expert Winn Schwartau has framed his warning for a potential cyberattack in these words:

> Historians claim that the devastation at Pearl Harbor in 1941 need never have occurred…Somewhere in the command structure, though, the belief was that the new fangled radar contraption was not reliable….The rest is history but we're still not listening [on cyberthreats].[38]

You ask for the circumstances and results of any historical precedent. In the case of Pearl Harbor, the results were to cashier the military officers whose names were consigned to ignominy for all time. Some minor research of the period recount these circumstances:

> One author who believes Admiral Kimmel was directly responsible for the disaster at Pearl Harbor is Henry C. Clausen, who served as a Special Investigator for the Secretary of War in 1945. In his book Pearl Harbor: Final Judgement, Clausen charges Kimmel was guilty of "criminal negligence and dereliction of duty." (204) One basis for Clausen's charges against Kimmel was his failure to take appropriate actions and precautions after receiving various messages and intelligence reports which constituted war-warning messages…
>
> Like his naval counterpart, Admiral Kimmel, many authors have fingered General Short as a culprit in the Pearl Harbor disaster. In addition to Kimmel, Clausen charges General Short with "criminal negligence and dereliction of duty" in his book. (204) Despite Short's apparent lack of interest in learning about the Hawaiian command before his assumption of command, Clausen argues Short knew that his primary duty was defending the Pacific Fleet and Hawaii from attack. (300) Obviously, Short failed in his duty.[39]

[28A] http://www.avdigest.com/aahm/trquotes.html

[38] Winn Schwartau, *Information Warfare, Electronic Civil Defense*, Thunders Mouth Press, New York, 1996. p. 589-590.

[39] James Daniel Wojnarek, Western Washington University, http://www.ac.wwu.edu/~wojnarj/pearlharborrev1.htm

> Contrary to the popular impression, Admiral Kimmel and General Short were never formally charged with errors of judgment or dereliction of duty. There was never a court martial proceeding. He and General Short were relieved of their commands and, in early 1942, placed on the Retired list.
>
> Kimmel's superiors repeatedly advised him that there was no danger of torpedo attack, because, they were confident, the harbor's waters were too shallow and any airdropped "fish" would simply sink to the bottom (the Japanese solved this problem by affixing special fins to their torpedoes; U.S. Naval Ordnance did not think this was possible).[40]

While there was controversy over where responsibility for what happened at Pearl Harbor lie and Kimmel was eventually exonerated, the attack was partly a result of cultural lag wherein unfamiliarity with aerial bombardment, radar and the underestimation of the abilities of the Japanese ordnance, all contributed to the debacle.

It is popular in military circles to say that “we always prepare for the last war” due to the propensity to take the threat of the previous war and apply it as the focus of defense for a future war. Not to overly prolong this answer but, today, we see similar circumstances. Our utility planners have, in effect, received their “war warning messages” but like Admiral Kimmel at Pearl Harbor appear unready to react. We see cultural lag in infrastructure planning where we are told “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” and we need to place a special responsibility on those who ought to have their “antenna’s up” and “radar screens on” so they have some idea of how to “connect the dots”. While future plaintiffs probably can’t sue them in a civil court for dereliction of duty, the case for some form of negligence may be a possibility.

---

[40] Institute for Historic Review. Reprinted from The Journal of Historical Review, vol. 11, no. 4, pp. 431-467. http://www.ihr.org/jhr/v11/v11p431_Lutton.html

Q: But if a "digital Pearl Harbor" has not yet actually occurred, why should utility executives, planners, regulators et al. be concerned about it?

A: "Absence of certainty does not mean absence of risk"[41] is one good reason for concern. After all, Pearl Harbor (the location) did not become "Pearl Harbor" (the event) until it actually occurred. But, beyond that, there has actually been one recorded attack on an ISO. The account reads:

> For at least 17 days at the height of the energy crisis, hackers mounted an attack on a computer system that is integral to the movement of electricity throughout California, a confidential report obtained by the Los Angeles Times shows.
>
> The hackers' success, although apparently limited, brought to light lapses in computer security at the target of the cyber-attack, the California Independent System Operator, which oversees most of the state's massive electricity transmission grid.
>
> Officials at the Independent System Operator say the lapses have been corrected and that there was no threat to the grid. But others familiar with the attack say hackers came close to gaining access to key parts of the system -- and could have seriously disrupted the movement of electrons across the state.
> A report stamped ``restricted" shows that the attack began as early as April 25 and was not detected until May 11.
>
> The attack on the ISO's computer system apparently had the potential for more serious consequences, given that the hackers managed to worm into their computers at the agency's headquarters in Folsom, east of Sacramento, that were linked to a system that controls the flow of electricity across California. The state system is tied into the transmission grid for the Western United States.
>
> ``This was very close to being a catastrophic breach," said a source familiar with the attack and the ISO's internal investigation of the incident.[42]

While this attempt failed to bring down the grid, there are indications that there will be an increase in such activities and the potential for actual disruptions appears likely.

While not an electric grid incident, a water company in Australia had its system hacked by a former insider and according to the following account:

---

[41] Attributed to Dr. Jeremy Leggett, a former oil scientist turned environmentalist who brought property-casualty insurers into the climate change dialogue to support CO_2emissions reductions.

.. in April 2000, a disgruntled consultant-turned-hacker compromised a waste management control system and loosed millions of gallons of raw sewage on the town. The good news...is it took this former insider 46 tries to unleash the waste; the bad news is that those managing this critical infrastructure missed his first 45 attempts.[43]

There has even been some cyber activities reported with the August 14th Blackout. In spite of its inability to yet identify a root cause, the US-Canada Power System Outage Task Force draft study on the blackout has been quick to discount cyber problems as a direct or indirect cause of the August 14th event:

> The SWG [Security Working Group] acknowledges reports of al-Qaeda claims of responsibility for the power outage of August 1, 2003; however, those claims are inconsistent with the SWG's findings to date. There is also no evidence, nor is there any information suggesting, that viruses and worms prevalent across the Internet at the time of the outage had any significant impact on power generation and delivery systems. [44]

This being said, they have still failed (in their Chapter 8 specifically on physical and cyber aspects) to adequately explain reports in the press that may have prevented FirstEnergy Control Room personnel from adequately assessing their situation due to widely reported computer-related problems. These may have been related to computer viruses or worms including one very specific account:

> At one point, an engineer at the Midwest grid managing organization asked engineers at the Ohio utility, FirstEnergy Corp., to explain why they had not responded to a line outage reported sometime earlier and asked that they find out what was going on.
>
> "We have no clue. Our computer is giving us fits, too," replied a FirstEnergy technician identified as Jerry Snickey. "We don't even know the status of some of the stuff (power fluctuations) around us."
>
> A short time later, a technician at the Midwest Independent Transmission System Operators, the group that monitors the Midwest power grid, expressed frustration with FirstEnergy's failure to diagnose the problems erupting in their power system.
>
> "I called you guys like 10 minutes ago, and I thought you were figuring out what was

[42] Dan Morain, "Hackers Mount Attack on Power System, Report Says," San Jose Mercury News, June 10, 2001.
[43] The Truth About Cyberterrorism, Scott Berinato, CIO Magazine, 3/15/02.
[44] US-Canada Power System Outage Task Force: Causes of the August 14th Blackout. p. 93.

> gong on there," the MISO technician, identified as Don Hunter, complained, according to the transcripts.
>
> "Well, we're trying to," replied Snickey. "Our computer is not happy. It's not cooperating either." [45]

It should also not go unnoticed that the blackout came only days after the Blaster worm infected hundreds of thousands of computers and that the previous Slammer worm had infiltrated portions of the FirstEnergy system.[46] However, until this Task Force better identifies root causes and better addresses the cyber aspects of the episode, doubts still remain over cyber problems as one among a number of contributing factors. Even a tangential relationship would still be cause for great concern since financial markets could view any vulnerability of the electric infrastructure as a risky proposition for all businesses. That said, this one to two day event should have been invaluable in alerting the industry to the seriousness of what could transpire if a directed cyber and/or physical attack were perpetrated by skilled personnel. Dr. William Flynt, Senior VP of TRC Customer-Focused Solutions and a former U.S. Army, Lt. Colonel and "Red Team"[47] member in speaking of one exercise noted:

> Using terrorist best practices, it was trivial to achieve significant consequences… Threats were measured at a significant level which means a multi-state region at 168 hours or one week, secondary or tertiary effects continuing on…to fully restore a system to its original configuration, same robust capabilities, took between one year and 18 months…[48]

In describing another exercise he stated:

---

[45] H. Josef Hebert, Associated Press. *Calls Show Pre-Blackout Utility Confusion*. September 3, 2003.
[46] Krebs, Brian. *Hackers Did Not Cause Blackout.* Washingtonpost.com November 19, 2003.

[47] A "Red Team" refers to members of our own national security, military or infrastructure-knowledgeable personnel who test the vulnerabilities of critical infrastructures without inflicting actual damage.
[48] William Flynt, Ph.D., *Terrorism and the Electric Power Infrastructure*, Keynote Session, International Conference on Advanced Technologies for Homeland Security, UCONN, September 25, 2003.

We took a sworn police officer in the region to conduct a test. We put him in front of an actual SCADA terminal, operating system terminal control center. We gave him real data but put the terminal in a training mode so we wouldn't actually cause any blackouts as a result of our experiment. And this police officer was computer literate. He could use e-mail. He could word process but he had zero…in the way of experience with SCADA systems and he had no real knowledge of how to operate an electric power grid…And we found by putting him in front of these consoles that he was able to accomplish single handedly a regional blackout that I would say would rival what we saw last month [August 2004] in about nine minutes and forty seconds.[49]

IV. DISTRIBUTED GENERATION TO SUBSTITUTE FOR NEW TRANSMISSION LINES AS A METHOD BY WHICH TO LESSEN GRID VULNERABILITY.

Q. What is your definition of distributed generation?

A: Because of questionable statements made before the DPUC and the Energy & Technology Committee by the ISO-NE and Northeast Utilities (NU) on distributed generation, let me stress the criticality of the definition(s) of distributed generation. Unlike their witnesses, I will not provide you a self-serving definition of my own design but would defer to the official definitions provided by such diverse groups as the US DOE, Electric Power Research Institute, American Gas Association and the California Energy Commission which are as follows:

US DOE I

Distributed power is modular electric generation or storage located near the point of use. Distributed systems include biomass-based generators, combustion turbines, concentrating solar power and photovoltaic systems, fuel cells, wind turbines, microturbines, engines/generator sets, and storage and control technologies. Distributed resources can either be grid connected or operate independently of the grid. Those connected to the grid are typically interfaced at the distribution system. In contrast to large, central-station power plants, distributed power systems typically range from less than a kilowatt (kW) to tens of megawatts (MW) in size. (http://www.eren.doe.gov/distributedpower/sublvl.asp?item=definition)

US DOE II

"Distributed energy resources (DER) refers to a variety of small, modular power-generating technologies... DER systems range in size and capacity from a few kilowatts

[49] William Flynt, Ph.D. Op cit.

up to 50 MW. They comprise a portfolio of technologies, both supply-side and demand-side, that can be located at or near the location where the energy is used.", (http://www.eere.energy.gov/der/basics.html)

Electric Power Research Institute (EPRI) I

Integrating distributed energy resources. The new system would also be able to seamlessly integrate an array of locally installed, distributed power generation (such as fuel cells and renewables) as power system assets. Distributed power sources under 20 MW per unit could be deployed on both the supply and consumer side of the energy/information portal as essential assets dispatching reliability, capacity and efficiency. Today's distribution system, architecture, and mechanical control limitations, prohibit, in effect, this enhanced system functionality. (Electricity Sector Framework For The Future, Volume I. Achieving The 21st Century Transformation, Aug. 6, 2003. p. 29. Full study at: http://www.epri.com/journal/details.asp?doctype=features&id=671)

EPRI II

"Distributed resources are small generation (1kW to 50MW) and/or energy storage devices typically sited near customer loads or distribution and sub-transmission substations," EPRI, http://www.epri.com/targetDesc.asp?program=262184&value=03T101.0&objid=287595)

American Gas Association

Distributed generation (DG) is the strategic placement of small power generating units (5 kW to 25 MW) at or near customer loads. Situated at a customer's site, distributed generation can be used to manage energy service needs or help meet increasingly rigorous requirements for power quality and reliability. Located at utility sites such as substations, distributed generation can provide transmission and distribution (T&D) grid support and expand the utility's ability to deliver power to customers in constrained areas. Distributed generation technologies include such resources as industrial gas turbines, reciprocating engines, fuel cells, microturbines, wind-power, and photovoltaics. http://www.aga.org/Content/ContentGroups/Newsroom/Issue_Focus/Distributed_Generation.htm

California Energy Commission

"Distributed energy resources are small-scale power generation technologies (typically in the range of 3 to 10,000 kW) located close to where electricity is used (e.g., a home or business) to provide an alternative to or an enhancement of the traditional electric power system." (http://www.energy.ca.gov/distgen/index.html)

Please note that, as diverse and these groups are, in each of these definitions the upper limit is not less than 10 megawatts in size and frequently close to 20 MW with an upper limit of 50 MW in two instances. An absolutely critical point in the Stephen G. Whitley testimony of 5/1/02 concerning DG in Docket # 02-04-12 (at Attachment 4, page 42) is that while earlier acknowledging (at line 873) that microturbines range in size from 25 kW to 200 kW he chose the lower size limit to make his point that thousands of units would be required to be installed each year to make up 50 MW blocks of power. (At lines 880-881.) What he left unsaid is that it would require far fewer microturbines in the 200 kW range and he totally ignores the immense range of miniturbines and turbines over 200 kW up to 50 MW that can also be considered "distributive generation" under the above government and industry definitions.[50] At these larger capacities, DG of this size would not take many units (as he has consistently claimed for DG) to have some supposed significant effect.

At the Energy and Technology Committee Hearing pertaining to the August 14th Blackout the following exchanges by legislators and Mr. Whitley are also crucial to understanding the continued denigration of distributed generation that Mr. Whitley presents:

> REP. NARDELLO: Well, the reason I say that is it's key to the issue here because when Chairman Backer talked about distributed generation and all of that, the greater systems and the bigger systems that we build I have concern that they will all cascade and fall. I mean, I have concerns about that. If we put in distributive generation where we can and I know that we can't do it everywhere and use those mechanisms and decentralize the system, there's less chance of these collapses, I would think. Am I correct in that?
>
> STEVEN WHITLEY: I disagree. I think what's needed -- we need distributed generation, but that's not going to solve our problem. We need a robust transmission infrastructure to keep the lights on in New England. We've got the generation, we need the transmission system so that we can keep the lights on. It's fundamental.
>
> REP. NARDELLO: But won't the DG be sited closer so that we won't have to go through the lines as much?

---

[50] Many small simple cycle and combined cycle turbines might be appropriate for individual businesses or industrial parks where they might also have a need for combined heat and power to provide efficient utilization of increasingly expensive and tight natural gas supplies

STEVEN WHITLEY: That's a what if. And it hasn't been so far. We've thrown a lot of money at it. It takes a lot of DG to make up for a 345 kV transmission, I mean lots of it….
REP. MEGNA: Thank you, Madam Chair. Mr. Whitley, is there an active load response program in southwest Connecticut? I know for a few years you were working on one.
STEVEN WHITLEY: There is and it's worked fairly well. We do have some demand response in southwest Connecticut. Part of that response that we're counting on are these two emergency generators that are pulled in on trailers to burn oil. That's part of the program.
REP. MEGNA: Is that the program or part of it?
STEVEN WHITLEY: That's part of it. That's the major part of it.[51]

While not explicitly identified, the "two emergency generators pulled in on trailers" Whitley identified are supposed to be the TM-2500 GE gas turbines at Waterside Crossing each of which approximates 23 megawatts--<u>well within many of the definitions provided of "distributed generation" presented herein</u>. So, while Mr. Whitley denigrates the ability of "distributed generation" to aid in the congestion problem on the one hand ("It takes a lot of DG to make up for a 345 kV transmission, I mean lots of it,") he credits what he does not even recognize as distributed generation in the form of those two turbines (as recognized by government and industry experts as DG) as being a "major part" of his own load response program. This questionable knowledge of the basic definitions of DG by one in a position of authority and supposed expertise calls into question the validity of his "one-note solution" to the congestion problem i.e. the 345 kV lines. Furthermore, this limited expertise and scope of leadership argues against ISO-NE being allowed to transition from an ISO into an RTO which appears to potentially only centralize and consolidate command and control power in the system even further.

---

[51] Committee hearing on the August 14th, 2003 Blackout held on September 11, 2003 at the CT LOB. Transcript at http://www.cga.state.ct.us/2003/ETdata/chr/2003ET-00911-R001330-CHR.htm

A similar inference on DG is also made in Mr. Richard Soderman's (NU) testimony in Docket # 02-04-12 (at page 4) where he states that: "However, the Department should recognize that C&LM, as well as emerging distributed generation technologies, while attractive, will only supply a small amount of load reduction relief, and they cannot and should not be considered a viable substitute for the transmission projects." He repeated this allegation in response to a question by Commissioner Kelly at the 5/8/02 hearing where, as one of a panel, he said DG was not possible as a practical solution in the time span allotted. Indeed, the three TM 2500's being used for the SW CT LRP mentioned previously, while not ideal, are exactly one such DG solution albeit of a more temporary nature. While some technologies such as fuel cells and photovoltaics require further development and cost reductions, there is sufficient turbine product availability now in large enough sizes to offer more than a "small amount" of load relief without having to install "thousands" of them. Even the seemingly far more expensive renewable technologies have their positive attributes that make them worthy of consideration.

Stacking the definitions in this way is a great disservice to better meeting certain societal needs e.g. energy security.

Q. Do you believe this bastardization of the definition of "distributed generation" has affected decisions makers?

Yes, I do. One interview by Connecticut Business Magazine (CBM) reveals the following dialogue with DPUC Chairman Donald Downes:

> **CBM:** Speaking of southwest Connecticut, is distributed generation part of the solution to the energy crunch in Fairfield County?..
>
> **Downes:** ... The biggest problem in Fairfield County — by no means the only problem — is that the wires down there are too small to carry power over distances

> where it's needed. Distributed generation will help in some ways, because what you're doing is generating the power on-site, so it doesn't need transmission lines.
>
> But it isn't that simple. For instance, the Bridgeport Energy Partners plant is an 844-megawatt combined cycle gas plant. If you were going to replace that with fuel cells, it would take 422 fuel cells. I don't think the people of Fairfield County realize that this would mean 15 or 20 of these per town…
>
> **Downes:** So fuel cells are not a perfect arrangement although… they certainly are useful, and absolutely a piece of the solution. What people have to realize is that there's no magic bullet, no single answer…[52]

While the Chairman handles the question well in recognizing the need for more than one solution--"no magic bullet"--he has been left with the impression that: 1) it might take 844 MW of capacity in DG to solve the problem and 2) this might need to come in increments of 2 MW. Again, there are numerous gas turbines available in the 5 MW to 50 MW range that could meet the needs without requiring 15 to 20 in each town. In the future, when fuel cells do meet certain price targets and more modular sizes (say 2 to 7 kW for home use), one could easily foresee a very large number in each town providing even greater resilience.

Q: What attributes of distributed generation may make it attractive?

A: There are numerous attributes in the many technologies that make up what we call distributed generation that can make it attractive to business and industry as well as grid planners and owners. These include but are not limited to:[53]

Reliability. One of the major advantages of distributed generation is its ability, <u>in conjunction with and parallel to</u> grid-supplied power, to provide reliability in the 99.9999% range required by many businesses who are now dependent upon digital technologies. For this reason, placing the DG on the customer side of the meter holds

[52] "How Will Connecticut's Transitional Standard Offer Affect Your Business?" Connecticut Business Magazine. Sep./Oct. 2003. p.76.

special appeal and not, as Mr. Anthony Vallillo, as a panel member at the hearing on 5/8/02 in Docket #02-04-12, alluded to for placing it at or near a substation where faults may present a greater problem. Running the systems in parallel where the DG does not ship power to the grid can also alleviate some of these problems. Since the owner of the facility would pay the majority of the cost of the unit, any "subsidy" paid to entice the owners of digitally dependent businesses would be minimal compared to the cost of lines as a first step. Additionally, all players would benefit since, like C&LM, use of the DG would provide benefit by lowering the market clearing price for all system users.

Power Quality. Like reliability, power quality is an absolute necessity for digitally-dependent businesses since any aberrations in power may be enough to lose valuable data or the programming of computers resulting not just in a momentary glitch but hours or days lost in having to reacquire data or in reprogramming.

Modularity. In the past, in order to realize economies of scale resulting in high efficiencies it was necessary to build steam turbines of 1000 MW or more which often entailed billion dollar expenditures and produced overcapacity situations with large rate increases until loads caught up. The modular nature of distributive technologies allows for more perfect load matching which avoids this situation of overbuilding and overspending and the risk of tying up capital in such costly projects which may be underutilized and not produce income to match the debt payments.

Deferral of Transmission and Distribution Costs. Americans' demand for electricity is growing at almost two percent per year, but the power grid is expanding at

[53] These are attributed to numerous people in the DG field including, Lovins and Lehmann, Fred Gordon, Joe Chaisson, David Andruus, Howard Brown and others.

only half that rate.[54] In many situations, distributive technologies can offer a lower cost option than traditional transmission and distribution upgrades such as substations or new high voltage lines. This lower cost option is best realized when those in the private sector elect to install DG on the customer side of the meter for power reliability/quality reasons and reduce the load on the grid by relying on it as the primary source but runs in parallel with the grid. In this way the ratepayer is relieved of having to pay the total cost of large transmission projects. It may be necessary for a utility to pay an incentive to such a customer, much as they do for C&LM programs, but this can benefit all ratepayers and the Department should consider allowing a bonus rate of return on such company expenditures where they can be shown to be the least-cost solution. Mr. Anthony Vallillo noted during the panel of the 5/08/02 Hearing for Docket #02-04-12 that distributed generation requires a "public subsidy." This is certainly true of some DG and many other emerging technologies but the Council should be mindful that the development of the gas turbine as we know it today required huge military subsidies that continue to this day.[55] Additionally, any transmission line that is installed, in effect, receives a 100% "subsidy" from the ratepayers who entirely pay for it. In addition, the largest subsidy any company can enjoy is being a state-chartered monopoly, such as a distribution company.

Reduced System Losses. There is less line losses with generation closer to points of use. When electricity is transported over long distances and in areas where there may not be sufficient line capacity to accommodate increased loads, line loses can account for 6-8%; we are led to believe significantly more in congested areas. Distributed technologies can all but eliminate these losses. In comparing large central stations to

[54] Charlotte Legates, "Will WAM-ing Solve the BANANA Problem?" Energy.com. March 2, 1999.

distributed units it is important to account for such losses since not doing so provides an inappropriate comparison.

In Docket #02-04-12, Mr. Stephen Whitley's testimony of 5/1/02 (at Attachment 4, page 42) says that microturbines have low efficiency (25% to 29%) unless the exhaust is used on-site for other applications. Since lines losses from the central system are not mentioned, this is an inappropriate comparison as the fleet average of the central station plants in the ISO-NE territory is probably at a similar level after line losses are accounted for. Since the ability to use the full thermal load of large centralized plant (~300 MW) for on-site use would most likely not be possible, they are further disadvantaged compared to microturbines where the output is more likely to match local applications such as heating and domestic hot water for fast food restaurants.

Mobility. Distributive systems have the flexibility to be moved to a new location if loads do not develop or decrease over time or a total operation needs to be moved. This is exactly what is being exercised in the use of the three TM-2500 units supplying 69 MW of power for use during summers in the SW CT load pocket. It is my original understanding that after the summer peak period had expired, these units were to have been moved to another location where they have a higher value during our winter season.

Low Operations and Maintenance (O&M) Costs. Some DG have low O&M costs. Photovoltaics have no moving parts and therefore require little maintenance. Fuel cells have few moving parts to replace but currently require expensive periodic stack rebuilding. And even microturbines, with some moving parts, may have lower operating and maintenance costs than large traditional Rankine cycle generating systems.

---

[55] See *The Gas Turbine Diatribe* which highlights the subsidy history of gas turbine development from 1903 on.

Project Scale vs. Technology Risk. With smaller, distributed technologies there is less investment risk in placing large amounts of capital in larger, soon-to-be obsolete technologies. For instance, some large new gas plants have been built in areas where there is electric transmission congestion reducing their ability to sell power and endangering their economic viability. Small distributed sources used on site do not share this risk.

Low Financial Risk. By definition, there is less financial risk with small-scale projects than with large ones. Lenders take a much lower risk in investment into numerous but small distributive projects.

Less Regulatory Risk. There is less risk of regulatory changes for the short planning and installation cycle of a distributive technology than for larger, centralized longer term projects where air emission or siting requirements might change during the process.

Lower Fuel Diversity Risk. Since many of these new technologies can use multiple fuels or renewable energy sources there is risk reduction by diversifying the fuel mix away from sources which are either in short supply at any given time or under control of nations which may not share democratic values. Even where large reserves are domestically available, such as with natural gas, there is still the threat of disruption and escalating price pressures.

Ease of Siting. It has become increasingly difficult to locate large power plants and transmission facilities and the siting process can take many months if not years if oppositions arises. Many environmental and community groups generally oppose such projects if they perceive them as hazards to health, environment or property values. It is generally easier to win public acceptance for small-scale distributed and renewable energy facilities.

Short Lead Times. Shorter lead times mean fewer financial uncertainties. Since distributed technologies are built in the factory rather than on-site, there are fewer risks associated with lead times which, in the case of larger nuclear plants, have sometimes stretched out to 13 years from inception to completion. This reduces financial uncertainty and the time gap between when a unit is financed vs. when it begins producing income.

Fuel Cost Insensitivity. Because distributed generation can make use of multiple fuels or renewable energy, it will not be as subject to fluctuating fuel price risk as are many less efficient competing options. Natural gas prices have gone up in tandem with rising oil prices in the past years as well as due to an increasing number of new centralized power plants using it as their primary fuel.

Incentives from Deregulation. Deregulation (or restructuring as it may be more correctly termed) legislation has, in many states, mandated a system benefits charge that creates funds which are designated for use in furthering renewable energy and demand-side management technologies and practices. It may be possible to access some of these funds for installation of systems used for power reliability, quality or disaster preparedness purposes.

Many states have also instituted "renewable portfolio standards," which require providers of electricity to supply a certain percentage of their power from renewable sources, some of which could be distributed resources.

Environmental Improvement. Many distributive technologies result in low emissions of criteria pollutants. They also generally produce lower greenhouse gas emissions than traditional electric generation.

Q. How can distributed generation lead to reduced grid vulnerability?

A: There are at least three major way in which DG can lead to reduced grid vulnerability. 1) By physically dispersing the location of small, modular generators mostly on the customer side of the meter, not only is there a physical resiliency advantage but it also allows for some continued operation, perhaps within what is termed a mini-grid, if the overall transmission system has been disrupted either physically or by cyberthreats. Actually, the Electric Power Research Institute (EPRI) holds the same view when they state:

> **Adaptive islanding.** Following a terrorist attack or major grid disruption from natural causes, initial reaction will focus on creating self-sufficient islands in the power grid, adapted to make best use of the network resources still available. To achieve this aim, new methods of intelligent screening and pattern extraction will be needed, which could rapidly identify the consequences of various island reconnections. Adaptive load forecasting will also be used to dispatch distributed resources and other resources in anticipation of section reconnection and to help stabilize the overall transmission-distribution system. [56]

2) By locating the distributed sources closer to the place of use, it minimizes the importance of transmission which is the major point of vulnerability. This is confirmed by James Castle, manager of operations at ISO-NY who "said the system was usually operated by running the cleanest and least expensive generating stations. But the system could be less vulnerable if plants close to the high demand cities were started up, to minimize the importance of transmission lines."[57] Distributed

---

[56] Electricity Sector Framework For The Future, Volume I, Achieving A 21st Century Transformation. Electric Power Research Institute. August 6, 2003. p. 31.

[57] Op cit., Wald.

generation takes it a whole step further and also adds significant generation that is not only redundant but dispersed; both required for survivability.

3) By diversifying the mix of fuels/technologies used by the distributed units there is safety from disruption of any one fuel source. Natural gas which is gaining in use has the potential to become a fuel "monoculture" and over-reliance on it by as much as 60% by 2020 as per the Siting Council report does not bode well for resiliency issues.

It is noteworthy that in December 1989, the gas companies <u>twice</u> ran full page ads[58] in the Hartford Courant asking people to curtail their gas use during a period of extremely low temperatures. At that time the use of gas for electric generation was almost non-existent. In spite of multiple new pipelines, with the added new gas-fired generation, a similar event now accompanied by a disruption either purposely or from natural causes might have the potential to force a decision on who would receive gas for heating vs. electricity well noting that most gas-fired heaters now require electricity in order to operate. This would not be a pleasant decision for any Governor to make.

Q: Won't adding new transmission lines or placing lines underground also decentralize and reduce grid vulnerability?

A: To a degree both add some security in that one adds some redundancy while the other adds some "fortification" but is best thought of as building a Maginot Line type of defense as France hoped to use after WWI to keep German armies from invading.

Unfortunately, due to their cultural lag, the French did not envision the use of fast moving Blitzkreig tactics that rendered the Maginot Line not only costly but useless.[59]

---

[58] Available upon request.

[59] The Maginot Line was a powerful line of defense with a vast, dynamic, state-of-the-art, ultra-modern defensive system. Most of its components were underground, where interconnecting tunnels stretched for miles. There thousands of men slept, trained, watched, and waited for a war that never came. It was powerful and supposedly impregnable, yet it failed to save France from a humiliating defeat in 1940. In May 1940 Hitler simply chose to ignore it.

The same is true of redundant and underground lines, they miss a critical point in the change in warfare. The problem with additional/underground lines is that neither alters the main problem which is they still maintain a highly centralized system. Again, in cyberwar, redundancy, alone, is not enough to provide resiliency, it must also be decentralized. Lovins and Lovins define the weaknesses of centralization (in terms of physical vulnerability but applicable to cyber):

Today's predominantly centralized energy systems:

- consist of relatively few but large units of supply and distribution;
- compose those units of large, monolithic components rather than of redundant smaller modules that can back each other up;
- cluster units geographically, for example near oilfields, coal mines, sources of cooling water, or demand centers;
- interconnect the units rather sparsely, with heavy dependence on a few critical links and notes;
- knit the interconnected units into synchronous system in such a way that it is difficult for a section to continue to operate if it becomes isolated -- that is, since each units operation depends significantly on the synchronous operation of other units, failures tend to be system-wide;
- Provide relatively little storage to buffer successive stages of energy conversion and distribution from each other, so that failures tend to be a abrupt rather than gradual;
- Locate supply units remotely from users so that the links must be long…;
- Tend to lack the qualities of user-control ability, comprehensibility, and user independence. These qualities are important to social compatibility, rapid reproducibility, maintainability, and other social properties...important...to resilience.[60]

Q: Won't an upgraded transmission system enhance the ability to use distributed generation rather than inhibit it?

A: Not really. Among the reasons why:

[60] Lovins, Amory B. and Lovins, L. Hunter, Brittle Power, Energy Strategy for National Security, Brick House Publishing Co. (Andover, MA) 1982. P. 218.

1) It will not aid in the use of DG which is best used on-site running in parallel with the grid for reliability and power quality attributes rather than transporting it over any large distances. As such, DG does not benefit from construction of such lines.

2) Societally, if you place a tremendous amount of funding into these transmission upgrades in the way they are currently planned, that funding is no longer available for competing technologies; in this case distributed generation where utilities could provide some incentives for facilities to use DG much as they do with existing C&LM programs.

3) Because transmission lines such a large investment into long-term infrastructure, it locks society into a future where newer, more resilient technologies may be disadvantaged and continuing the payment for that infrastructure provides the justification to create arguments to keep new, competing technologies out. This might take place through institution of an exit fee or discriminatory policies toward interconnection and standby rates. (See following question for remarks on an exit fee.) In many respects my objections come down to an ordering of events. I see the C&LM coming first as they are the lowest cost and least objectionable. I suggest the distributed generation route next since large portions will be paid for by the private sector. To put the large transmission line build-out first means there may not be discretionary funding for the other vital portions of an adaptive grid. The EPRI study appears to recognize what both ISO-NE and NU have neither recognized or articulated in any meaningful way:

> A portfolio of innovative technologies, such as those described in this report, can comprehensively resolve the vulnerability of today's power supply system in terms of its capacity, reliability, security and consumer service value. These "smart technologies" will also open the door to fully integrating distributed resources and central station power into a single network, in a manner than can reduce system vulnerability rather than add to it—as is typically the case today—while also steadily improving the efficiency and environmental performance of the system.

> Lack of technical innovation strongly reflects the state of uncertainty in the electricity sector. Technology decisions are largely driven by the management of existing assets, with particular focus on reducing cost and reducing/hedging risk. Capital expenditures as a percent of revenue are at an all-time low, and operating and maintenance budgets remain extremely tight at most utilities. There is little incentive for introducing new technology when the recovery of investment is so uncertain.[61]

ISO-NE and NU do not, to my limited knowledge, actively put forward in their transmission plan a strategy that systematically provides a blueprint for this "portfolio of innovative technologies" but, rather, only the single solution of the 345 kV line and it appears to pay no heed to energy security considerations.

Q: Won't a proliferation of distributed generation promote a condition where, as more entities go off the grid, others will be left on and pay a larger share that may necessitate an exit fee?

A: This is not just a simplistic black and white issue with no shades of gray. There is certainly credibility to the point that those left on the grid could end up paying more if DG is not implemented in a meaningful way. Yet, to penalize technology through an indiscriminate exit fee could severely hurt the competitive position of the state to attract businesses that require high reliability and high power quality that the grid is not capable of supplying by itself. There are many shades of gray in the exit fee issue and let me suggest that the following alternatives be further investigated:

First, there is the potential to place the exit fee on the gas going into the distributive generation units since this would reward efficiency (someone at 40% efficiency in effect pays less than someone at 30% efficiency.) A combined heat and power project at about 85% efficiency might pay very little in this way and we ought to

[61] Electricity Sector Framework For The Future, Volume I, Achieving A 21st Century Transformation. Electric Power Research Institute. August 6, 2003. pp. 4 and 18.

encourage efficiency--not discourage it--for numerous reasons including some of the shortages we have seen.

Second, make it so that it might only apply to units over 50-200 kW (or whatever size can be agreed upon.)

Third, it might not kick in until a total of 100 MW (or 200? 500? etc?) was put in place. In this way you have at least rewarded the early adopters by mitigating investment risks for them.

Fourth, no fee would be charged on units placed into locations where distributive generators would relieve more costly T&D upgrades. If you consider other location sensitive exemptions from an exit fee, you may want to add: A) nursing homes B) people on medical conditions requiring electricity C) wastewater treatment plants so they don't have to overflow and pollute during natural disasters D) natural disaster shelters and public safety (first responders) facilities E) use where lack of high reliability and power quality would hurt economic growth.

Fifth, no exit fees on renewable energy sources of any size.

Finally, and maybe most important as a concept, why not take the electric usage of December 31, 1996 (same date as used as baseline for the standard offer price reduction) and use it as a baseline for electrical usage.

Then, allow distributed generation without an exit fee for increased amounts of electric usage above that baseline. This can be worked backwards into megawatts of capacity so the number of distributed generation megawatts allowed without an exit fee can be computed each year.

This is a self- balancing system which would have no losers since it maintains the same amount paid for the SBC and CTA and T&D as we had at the baseline time point.

V. A SIX POINT CYBER-DEFENSE PLAN

Q: Do you have any suggestions on what we may need to do to make the grid more resilient and why you see them as necessary?

A: Yes, I do. I would suggest the following six points be considered in revamping the way we think about the grid:

1) Large new, expensive transmission plans by utilities across the nation to alleviate power congestion further centralizes energy and may make the country vulnerable to cyber and physical attacks when there are alternatives that can mitigate much of this problem.

Transmission upgrade plans should be re-examined from a national security perspective before they are cast in stone since they can set the standard for a generation and lock in older technologies as some utility monopolies have in the past. This may mean bringing in new players who are not constrained by traditional regulatory and/or utility thought patterns or profit motivations--such as insurers who may also be able to mitigate business interruption losses via use of DG.

2) Use of load management and small, fuel diverse generators that are more widely distributed have the potential to provide a more robust system that is less vulnerable to physical and cyber attacks and should be considered as alternatives. They should be considered first in the order of battle.

3) Because many Connecticut firms produce these distributed generators such as gas turbines (or their components) and fuel cells, this could provide a major economic boost to make up for lost aircraft engine sales due to reduced flights as one effect of terrorism.

There are existing State financial mechanisms and funds that might make them even more economically attractive.

4) Since these distributed generators are most often paid for and placed on customer premises to insure power reliability and quality, the societal cost may be less since facility owners will pay for a large share rather than ratepayers footing the entire bill. In addition, the National Science Council's Study previously cited has made the recommendation that use of homeland security funds for funding distributed generation to maintain key loads would not be inappropriate:

> Today there is a growing interest in distributed generation —generators of more modest size in close proximity to load centers. This trend may lead to a more flexible grid in which islanding to maintain key loads is easier to achieve. Improved security from distributed generation should be credited when planning the future of the grid….Recovery of the invested funds through rate mechanisms or in some part through homeland security funding must be examined.[62]

While it is unclear whether EPRI is literal in its meaning of "incentive" as used below, they generally seem to share this opinion with the National Science Council:

> Protecting the nation's power infrastructure has a strong public-good dimension, and a robust federal "homeland security" incentive will be needed from the outset. Investments made for such essential infrastructure security must be immediately and fully recoverable. [63]

But this funding is far from certain as an even more recent study by the Council on Foreign Relations on lack of funding for emergency responders makes clear. Former Senator and security expert Warren Rudman is Chair and cybersecurity expert Richard Clarke, cited earlier several times, is Senior Advisor. That report states:

---

[62] *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.192. 2002.

[63] Electricity Sector Framework for The Future, Volume I, Achieving A 21st Century Transformation. Electric Power Research Institute. August 6, 2003. p. 7.

> Estimated combined federal, state, and local expenditures therefore would need to be as much as tripled over the next five years to address this unmet need. Covering this funding shortfall using federal funds alone would require a five-fold increase from the current level of $5.4 billion per year to an annual federal expenditure of $25.1 billion.[64]

Any forward looking homeland security strategy would seek to use some of these funds for distributed generation for these first responders and to maintain other critical services such as hospitals, communications and transportation. If co-located in areas of high electric congestion, they would concurrently serve two important yet unrelated purposes.

5) Because many distributed generation units are extremely clean and small, this option for congestion alleviation may be quicker to implement due to less need for environmental and other regulatory oversight being required. In the case of certain fuel cells, both Massachusetts and California have blanket environmental emissions approval.

6) Utilities should be allowed to ratebase any incentives payments to drive the private sector toward demand-side, distributed technologies up to 25 megawatts in size. There should even be consideration of allowing them to build and own such facilities in a step backwards from deregulation to provide them incentive not to oppose alternatives that are in the best interests of the nation. This would take a page from the Netherlands that allows utilities to build combined heat and power facilities in that nation and has resulted in 40% of the nation's power being supplied in that manner.[65]

---

[64] *Emergency Responders: Drastically Underfunded, Dangerously Unprepared*. Report of an Independent Task Force Sponsored by the Council on Foreign Relations. July 2003.

[65] James Lucky, *Distributed Power Dutch Style*, Energy Markets, June 2001, p. 8.

In addition to the aforementioned points, I would further suggest that the following steps also be taken to facilitate the required change in thinking that must accompany making the grid more resilient:

- Decouple utility profits from sales.
- Institute least-cost transmission and distribution planning as implied by PA 98-28, Section 52(e).
- Institute full performance-based ratemaking that provides rewards for least-cost alternatives, fuel diversity, modularity and survivability.

VI. ADDITIONAL QUESTIONS THAT REGULATORS SHOULD ASK

Q: What other questions should regulators be asking the FERC, the ISOs and the utilities?

A: I would begin by asking some rather pointed questions to those at the highest level and working down. These might include:

- Are they aware of the potential cyberthreats to the grid in their multiple forms?
- If aware of the threats, what actions have they taken with the existing system to protect against them?
- Have they examined the system structure itself and forward-looking designs to make the system more resilient?
- What will formation of RTO’s do in terms of energy security?
- To whom does the ISO owe primary allegiance and accountability?
- Does this drive power line projects over other alternatives and other considerations such as energy security?

- How does this allegiance influence their policy on mitigating threats? How are the considerations balanced?
- How much power (planning, political, etc.) should be surrendered to the RTO, the ISO by the states and where does liability lie if the RTO or ISO do not adequately address energy security considerations?

VII. CLOSING STATEMENT

Q: Do you have a closing statement?

A: Yes. I believe I have provided a case showing that enough current and former officials and other experts believe that cyberthreats to the energy infrastructure, including and in particular, the electric grid, presents a credible threat.

Evidence is strong that the reaction to this threat must be addressed by partnerships in the public/private sectors from planning through to construction of a more resilient system.

Expectations that the government alone can protect the critical infrastructure once it is built are extremely ill-founded. It behooves the electric power industry, its regulators at all levels and others involved in the decision-making process to carefully examine the future liabilities associated with failure to integrate the best available information that incorporates energy security concerns. In essence, to "connect the dots."

Existing and well-proven, as well as new technologies, can be used to provide a more resilient grid. Construction of only those transmission facilities as a first step on a purely "business-as-usual" basis can lock us into an electric Maginot Line for decades to come and deprive us of monetary resources that might have otherwise been used to our mutual benefit. In retrospect the building of those lines and their motivation could be looked upon as imprudent at best and negligence at the worst and leave all parties open to future suits by numerous aggrieved parties including the insurance industry who pay business interruption loss claims.

ISO-NE and NU have offered only one portion of what should be a far more comprehensive plan that makes energy security/resiliency in he the form of C&LM and distributed generation full partners along with increased transmission capacity for long distance power/monetary transactions. I believe it is time to "recess to reassess" and suggest that they, and the Siting Council, heed the advice offered by EPRI when they note:

> No one can solve the problem alone, and no single solution exists. With so many factors converging at one time on the electricity sector, it appears that the only way forward is for all stakeholders to find the will and the means to move on a broad front at the same time, as a matter of overriding mutual and national self-interest. Individual movement need not be in complete concert, however, because different pathways can lead toward the same destination.[66]

[66] Electricity Sector Framework For The Future, Volume I, Achieving A 21st Century Transformation. Electric Power Research Institute. August 6, 2003. p. 22.

Joel N. Gordes
97 Eno Hill Road
Winsted (Colebrook), CT 06098
Ph/fax (860) 379-2430
jgordes@earthlink.net
http://home.earthlink.net/~jgordes

Work Experience:

Energy Consultant **1995-Present**

Principal of Environmental Energy Solutions, an energy consulting firm involved in multidisciplinary aspects of energy, environment and economic development.

Acts as Technical Coordinator [administrator] of the Energy Conservation Management Board set up by the state's deregulation legislation. The Board advises the DPUC on the expenditure of over $87 million dollars annually in funds for conservation, load management and distributed resources.

He also serves as the Executive Vice President of the New York Solar Energy Industries Association (NYSEIA) in what is the 8th largest economy in the world and the second largest state by population in the nation. NYSEIA is comprised of over 70 members involved in the design, promotion, manufacturing and installation of renewable energy systems.

Consults to the Connecticut Clean Energy Fund, a $24 million per year fund to advance renewable energy technologies and use in Connecticut. Aids in crafting of their fuel cell and photovoltaics RFPs and is a member of their corresponding evaluation committees.

Provided technical reports on new concepts employing tidal power and ocean wave power to the Massachusetts Technology Collaborative, the agency tasked with developing the renewables industry under restructuring. Also provided information concerning military use of PV, use of PV in disaster mitigation and how renewables may have been useful in the January 1998 ice storm.

Selected by the Conservation Law Foundation in 1996 to consult to the Rhode Island Renewable Energy Collaborative (RIREC) to aid in renewable energy program design and implementation in Rhode Island under their first-in-the-nation utility restructuring legislation. Was later retained directly to conduct in-depth analyses of markets for PV powered outdoor lighting (1998) and PV powered digital, wireless communications systems (1999).

Contracted in 1996 to work with Dr. Jeremy Leggett on the Oxford (UK) Solar Investment Summit process to promote market pull for photovoltaic technology through uniting of financiers, manufacturers and solar consumer blocks. Subsequently named consultant to Dr. Leggett's Solar Century project which has been instrumental in promoting insurance and financial community investment into photovoltaic technology as a method to mitigate global climate change.

Durational Project Manager **1993 - 1995**

Served as durational project manager under a two year contract to manage the section of the State Energy Office concerned with renewable energy and gas turbines. Responsible for policy initiatives, public outreach and staff supervision.

Supervised the formulation and operation, including the RFP, of the first two rounds of the New Energy Technology program (NET) designed to aid small businesses involved in energy products bring them to commercialization.

Technical Coordinator **1990-1993**

Consultant to the Conservation Law Foundation, Office of Consumer Council, DPUC Prosecutorial Division and the Office of Policy and Management, Energy Section for conservation programs offered by the United Illuminating Company in the collaborative process of conflict resolution.

Responsible for formulation and consolidation of positions for the design, implementation and monitoring and evaluation of energy conservation programs totaling as much as $14 million per year. Oversaw the activities of five additional consultants. Wrote and issued RFPs for sub-consultant services.

Legislator **1987-1991**

State Legislator from Connecticut's 62nd House district. Served on the Energy and Public Utilities Committee (Vice-Chair 89-91) , Select Committee on Housing, Finance , Revenue & Bonding Committee, and the Executive and Legislative Nominations Committee.

Responsible for laws and concepts pertaining to the use of energy conservation and renewable energy sources including:

Co-author of Connecticut's Global Warming Act containing many conservation measures. PA 90-219

<u>Utility bonus rates of return for conservation investments. PA 88-57</u>

Relamping of all State buildings with compact fluorescents resulting in $4 million in first year savings for state budget deficit reduction. PA 90-221

Solar Design Analyst **1984-1987**

Employee of the Connecticut Housing Investment Fund engaged in operation of the Solar Energy and Energy Conservation Bank for the federal government. Performed ASHRAE heatloss and passive solar load ratio design analyses (SLR) for 250 homes and administered over $400,000 in mortgage subsidies.

Administrator **1979-1981**

Administrator of the Connecticut General Assembly's Energy and Public Utilities Committee. Supervised all functions of the committee including liaison with federal and state agencies, legislators, interest groups, media and the public. Assisted in researching and drafting legislation. Principal investigator for DOE funded compilation of all energy incentive programs in Connecticut which cross-referenced availability by project type.

Sales Engineer **1977-1979**

Sales engineer for Solar Resource Division of L.R. Smith, Inc. Responsible for sales and marketing of solar energy equipment, system sizing, pricing, response to bids and analysis of systems to be added to the product line.

Heavy contact with architects, engineers and contractors. Lobbied for solar energy incentives at the state level on a part time basis.

Engineer **1976-1977**

Engineer for Solar Industries, Inc. performing R&D on evacuated tube solar collectors. Preparation of technical proposals to secure government funding. Completed designs and manuals for one of the first twelve systems eligible for $400 HUD grants in CT. Lobbied for solar incentives on a part time basis.

Military Service: **1968-1973**

Officer, United States Air Force. Flew 130 combat missions in the RF-4C Phantom II reconnaissance aircraft. Last rank held was captain. Awarded Distinguished Flying Cross and nine Air Medals. Parachutist (Airborne) rating.

Education: United States Air Force Academy, Colorado
B.S. 1968.
Hartford Graduate Center of Rensselaer Polytechnic Institute
Solar Energy for Buildings, 1976.
International Gas Turbine Institute of A.S.M.E.
Basic Gas Turbine Technology, 1993.

Professional Affiliations:

American Solar Energy Society (Since 1978)
Northeast Sustainable Energy Association (Since 1976)
Volunteers in Technical Assistance (Aid to third world nations)
Reserve Officers Association

Other :

Named 1988 Environmental Legislator of the Year by
Peoples' Action for Clean Energy
1990 Distinguished Service Award from the Council of Small Towns
Recipient of the 1992 Connecticut Environmental Award by Connecticut Fund for the Environment
Recipient of the 2001 NE Sustainable Energy Association's Distinguished Service Award
2003 PACE Solar Pioneer Award

Publications, Papers and Presentations

Energy Security: A Driver For DG--Looking at Local Perspectives. Presentation for the American Solar Energy Society. Austin, TX. June 26, 2003.

Assessing & Communicating Renewable Energy Benefits-Cyberthreats to the Grid: A Driver for DG. Presentation for the American Solar Energy Society. Austin, TX. June 25, 2003.

Rating the States for Energy Security. *Paper and presentation for the American Solar Energy Society Solar 2003 conference with Susan Gouchoe and Steve Kalland of the North Carolina Solar Center of UNC. Austin, TX.June 24, 2003.*

Energy Security: A Driver for Distributed Generation. Presentation for the Mid-Atlantic Solar Energy Conference. Trenton, NJ. June 5, 2003.

Cyberthreats to the Grid. Air & Waste Management Association of Connecticut. March 18, 2003.

National Security & the Power Grid. Presentation for NESEA Conference's Building Energy 2003. Boston, MA. March 13, 2003.

Distributed Generation: A Prime Driver for Solar & Other Renewable Resources. Presentation for University of Hartford School of Engineering Class. October 30, 2002.

An Update on Utility & Energy Infrastructure Security. Presentation for the Connecticut Power & Energy Society. Cromwell, CT. September 12, 2002.

Cyberthreats and Gird Vulnerability. Presentation for the InfoWarCon Conference. Washington, DC. September 5, 2002.

Distributed Generation: Insurance and National Security Implications. Presentation for the Ozone Transport Commission Annual Meeting. Essex Junction, VT. August 6, 2002.

Cyberthreats: A Major Driver for Distributed Generation. Paper for the American Solar Energy Conference Solar 2002. Reno, NV. June 2002.

Cyberthreats and Grid Vulnerability (Considerations in Rebuilding the Transmission System). Presentation to the Connecticut Department of Public utility Control. Norwalk, CT Town Hall. May 10, 2002. Also presented at the Solar 2002 conference in Reno, NV on June 18, 2002.

Power to Insure: Distributed Generation As An Insurance-Friendly Option. Presentation for the Northeast Sustainable Energy Association Tufts University Conference. March 21, 2002. Also given at the Earthday New York Conference: Rethinking the Built Environment. May 1, 2002. Also presented at the NESEA Rutgers Conference. June 27, 2002.

Cyberthreats to the Grid. For the Policy Working Group of the Energy and Technologies Committee. Hartford, CT. February 2002. Also given to the Connecticut Energy Advisory Board on March 5, 2002., to DPPUC Commissioner L. Kelly, CT DPUC on 4/29/02 and to Consumer Counsel Mary Healy on 5/8/02.

Energy Security: Protecting U.S. Sovereignty and Infrastructure. *Presentation for the Environmental and Energy Study Institute. Rayburn Office Bldg. Washington, DC. February 7, 2002.*

In addition to these and many other publications not related to energy security, from 1991 to 1993 he wrote a bi-monthly column pertaining to energy, environment and politics for the Torrington-based Register-Citizen, a daily paper in Northwestern Connecticut. Copies are available upon request.