STATE OF CONNECTICUT
CONNECTICUT SITING COUNCIL

| | | |
|---|---|---|
| RE: IMPLEMENTATION OF SECTION 8 | : | **Docket #346** |
| OF PUBLIC ACT NO. 07-242 AN ACT | : | |
| CONCERNING ELECTRICITY AND | : | |
| ENERGY EFFICIENCY | : | |

**November 25, 2008**
**Comments and Testimony**
**Toward Best Management Practices on**
**Energy Security Risks & Considerations**

**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. The EES office is located at 38 Brookmoor Rd., West Hartford, Connecticut 06107.

**Q: Summarize your qualifications to speak on energy security issues**.
A: Mr. Gordes of EES is an independent energy consultant with experience in energy efficiency, renewable energy, climate change as it affects the insurance industry and issues pertaining to energy security matters. He has been involved in the energy field for the past 33 years in a variety of capacities including active and passive system/home design, technical analysis, program operations, program design, strategy development, policy development, legislation and energy association management. EES has:

1) Training in military arts and sciences including unconventional warfare and has held a top secret clearance.
2) Been an invited speaker at the International Conference on Advanced Technology & Homeland Security to speak on cybersecurity issues
3) Been an invited speaker by NARUC 's Ad hoc Committee on Critical Infrastructure to present on cyber vulnerabilities of the power infrastructure. (Comm. Connie Hughes NJ BPU, Chair, 11/17/04)
4) Written popular articles, papers and presentations pertaining to energy security

EES's entry into the energy field in 1975 was based largely upon energy security motivations mostly concerning overdependence on oil from foreign sources. Mr. Gordes first noted the vulnerability of the electric grid to natural and man-made hazards as early as 1978 when he was first published on the topic. EES makes no pretense on having deep expertise in electric grid design or operation but does not believe this lessens the ability to observe flaws in the system and report on the observations of those who do have such expertise. In this respect, EES serves much in the role of a messenger. Some of EES's publications and presentations on energy security/resilience are provided at http://home.earthlink.net/%7Ejgordes/page8.html.

EES wants to stress that, today, Mr. Gordes is here as an individual on a pro bono basis and representing none of these or any other groups.

## II. INTRODUCTION, SCOPE AND DEFINITION OF TERMS

**Q: What is the purpose of your direct testimony?**

A: EES appreciates the Connecticut Siting Council's (CSC) sponsorship of this docket pertaining to the topic of Best Management Practices (BMP) for the Security of Siting Energy Facilities in Connecticut and the thought given to providing a baseline document. The purpose of the EES combined comments and testimony is to provide information the CSC might wish to consider for incorporation into its BMPs. EES notes these siting concerns should apply not only for selective generation and transmission assets in isolation basis but that the grid be viewed in a more holistic framework. Attention is required to the interactions of each transmission or generation addition upon the whole and any resultant effect(s) pertaining to grid security. This was generally noted in the EES motion for status as an intervenor and at least implied in the CSC Draft BMP (at p.2, A. Planning 3. Interdependencies). These comments and testimony will also address security aspects of the fuels used and the emergence of new threats all of which may contribute to the need for rethinking some fundamental assumptions. Where appropriate, this will include mostly consideration of planning and preparedness aspects of the BMPs but may address response and recovery as necessary. EES also hopes to demonstrate how perverse actions are sometimes taken in regard to security.

"The electrical power grid, a massively complex machine, the largest on earth, was recently acclaimed by the National Academy of Engineering as 'the most

significant engineering achievement of the 20th century'."[1] EES agrees with this assessment and is not anti-transmission line on a NIMBY basis but notes that security did not appear to be a primary consideration in the grid's development.

Section A, (Planning) of the BMP makes a vitally important point when it requests identification of security threats and vulnerabilities. Too often we use terms that may have vastly different meanings to others. While some have limited energy security to the narrow confines of oil dependence, EES sees at least five distinct security threats to the electric grid.[2] These include:

- Energy security in the form of fuel supply interruption/cost escalation
- Physical security of grid components (generation, transmission, distribution)
- Foreign dependency via disruption of globalized supply chains for critical grid components and minerals used in component manufacturing processes
- Cybersecurity threats including distributed denial of service, hacking, electromagnetic pulse, embedded codes in foreign sourced components
- A combined or "blended" combination of the aforementioned threats

Due to limited resource, EES can only comment in limited depth on these issues particularly on some less-often discussed aspects of fuel supply and foreign dependency issues relevant to the BMP's planning and preparedness sections that might impact critical infrastructure.

**Q: Isn't security more a federal issue not normally addressed at the state level?**
A: Normally this might fall under national security which would be handled at the federal level, however, in this case we have a direct mandate to investigate it in Sec. 8 of PA 07-242. Also, PA 03-140, AAC Long-term Planning for Energy Facilities, added the words "to promote energy security" to 16-50g. In addition, conflict has changed its nature, aims and targets over time from being purely for territorial gain and wealth to ideological struggles where winning "hearts and minds" is tantamount to "victory". Today, "victory" may take on yet another face where the adversary's economy may be the most attractive target. While proposed in a different context, the Eisenhower administration's National Security Council directive 149/2 recognized, "The survival of the free world depends on

[1] Steven G. Hauser. It's the Grid: Blueprint for the Future EnergyBiz M-A 2008 p. 23. Also see http://www.nationalacademies.org/greatachievements/List.PDF
[2] Other Parties/Intervenors are encouraged to add to this list.

the maintenance by the United States of a sound, strong economy."[3] The criticality of the economy was also foremost in an actual definition of Information Warfare (IW) provided in one early work:

> Most clearly, though, the distinctive feature of pure IW is that it can be so easily waged against a civilian infrastructure in contrast to a military one. This is a new facet of war, where the target may well be the economic national security of an adversary. In addition, though, we have distributed the capability to wage war.[4]

Under these ground rules, what better way to damage the US than to inflict unacceptable damage onto one major driver of its economy? The US electric sector is the prime target[5]. Schwartau, once again sums it up when he says:

> 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. [6]

Then-Red Team member, Ltc. William Flynt said much the same at an ISO-NE/ISO-NY sponsored conference:

> 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.[7]

Much of the siting and regulation of these facilities is done at the state level making this docket a legitimate venue for security considerations at this level.

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

> "The owners and operators of electric power grids, banks and railroads; they're the ones who have to defend our infrastructure. The government doesn't own it, the government doesn't operate it, the government can't defend it. .....the military can't save us."[8]

That being said, the government, through numerous boards, councils and agencies[9] can refrain from siting decisions that, in effect, might enhance the appeal of certain elements of the critical energy infrastructure for terrorist attacks. It is likely this has already taken

---

[3] Adams, Valerie L. Eisenhower's Fine Group of Fellows: Crafting a National Security Policy to Uphold the Great Equation. Lexington Books. 2006. p.30.

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

[5] See NYT article at chttp://www.box.net/shared/2h5b7zy9g5 citing this at an ISO-NE Conference in 2002

[6] Winn Schwartau, Information Warfare, Electronic Civil Defense, Thunders Mouth Press, New York, 1996. p. 43. Actually, the number of elements considered to be part of the "critical infrastructure" has increased to at least 8 and as many as 13 by some estimates.

[7] Matthew L. Wald, "Electric Power System is Called Vulnerable, and Vigilance is Sought," New York Times. 2/28/02. See http://www.box.net/shared/2h5b7zy9g5 for ISO NE/NY cyber conference.

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

[9] Often with very different if not conflicting agendas.

place. The prestigious Center for Strategic and International Studies (CSIS) echoes Clarke's sentiment when they say:

> At the same time, the United States Armed Forces cannot defend the nation against such attacks. Lines of defense and accountability often lie in the hands of individuals and smaller organizations…Yet such threats are poorly understood by those responsible for their prevention.[10]

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

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

A. Over the years, in conversations with some personnel connected with the some regulatory bodies and utility executives, EES has been unable to discern any deep familiarization with some of the topics of vulnerability; particularly to critical infrastructure supply chain problems or cyberterrorism/cyberwar. Most security concerns seem oriented toward preventing physical attacks. As often said in the military, "we always prepare for the last war". This can mean late recognition of newly emerging threats. EES would like to alert the CSC to some of them as much as possible within the context of the BMPs but outside them if necessary. The draft BMPs provide leeway in evaluation to address what is presented "as much as practicable" (BMP at p.1, para. 4) but also, EES assumes, the right, and even the responsibility, to go beyond to what is less predictable.

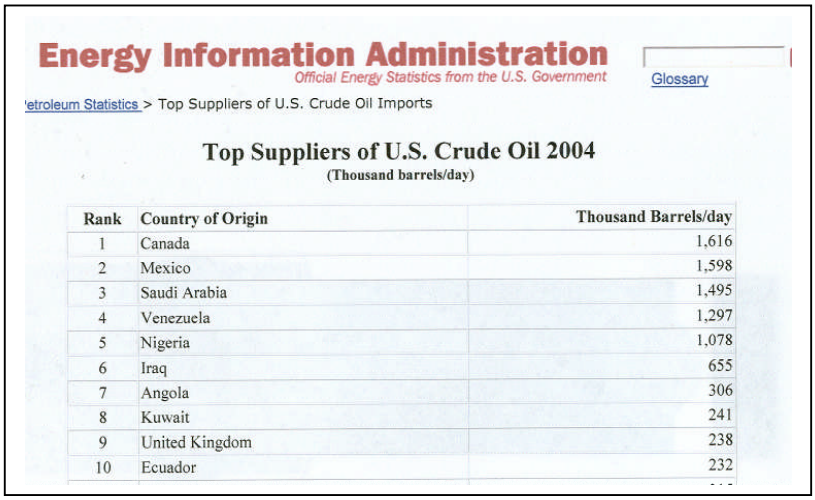
## III. FUEL RELATED ISSUES

[10] 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 do you see as fuel-related issues?**

A. Well, of course everyone knows we have a problem with oil but if you look at the actual kWh generated from oil for Connecticut it is a very small amount. According to ISO figures it is a mere ~4% by kWh while the CSC shows it as ~37% by capacity (MW). So we need to begin to express our usage in a more representative way which EES feels kWh does. While this decouples oil from large amounts of direct generation, it is still the basis of our entire society and is responsible for everything from the mechanization of agriculture that frees most of us from having to be farmers to the freedom of mobility we enjoy. Make no doubt about it, any reduction in access to oil or the quality of our supply will have deep impacts on all facets of life. This includes the electric grid as EES doubts we could survive at our current standard of living without the cheap, concentrated energy afforded by oil at this time.

The table immediately below shows from where we import our oil. Contrary to popular belief, we only import ~20% of our imports from the Middle East and imports are approximately ~60%-65% of our oil so only ~13% or so (possibly as much as ~18% with updates but still below common assumptions) of our total oil originates there. At some times it has been greater and will likely become so again.



Energy Information Administration

Official Energy Statistics from the U.S. Government

Glossary

etroleum Statistics > Top Suppliers of U.S. Crude Oil Imports

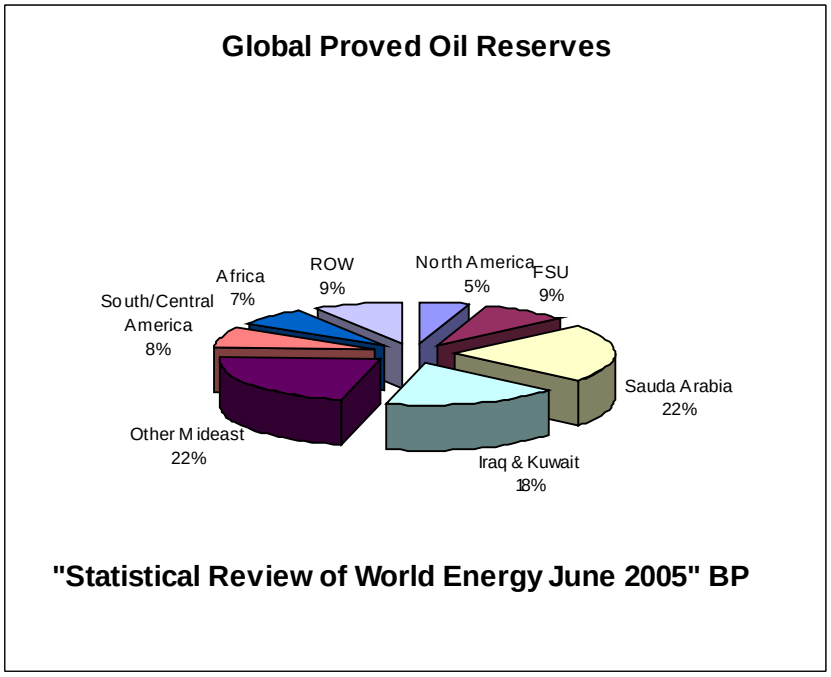
**Top Suppliers of U.S. Crude Oil 2004**

(Thousand barrels/day)

| Rank | Country of Origin | Thousand Barrels/day |
|---|---|---|
| 1 | Canada | 1,616 |
| 2 | Mexico | 1,598 |
| 3 | Saudi Arabia | 1,495 |
| 4 | Venezuela | 1,297 |
| 5 | Nigeria | 1,078 |
| 6 | Iraq | 655 |
| 7 | Angola | 306 |
| 8 | Kuwait | 241 |
| 9 | United Kingdom | 238 |
| 10 | Ecuador | 232 |

A good deal of our oil comes from our closest neighbors, Canada and Mexico, and while we may feel these supplies are secure, unintended consequences sometimes arise from seemingly unconnected actions. For instance, building a fence along the US southern border to keep out illegal immigrants might be perceived in Mexico far differently than in the US leading to some blowback -- one of the perverse results I

alluded to earlier. Looking at the list above, it would not take too many of these nations, (several of which might be considered "unstable") to attempt some disruptions to our oil flow. But those sources may be a less important factor today particularly since oil is traded on a global commodity market. The pie chart below page provides a better representation of our future if we do not drastically reduce oil use in the next few decades. What this shows us is that at least 62% of the world's proved reserves are located in the Middle East.




Even if we drill offshore and in the ANWR, EES generously notes the mean estimated reserves approximate 96 billion barrels according to the Mineral Management Service. However, since we use approximately 7.5 billion barrels per year, without a plan to transition to other sources after that runs out, our future will be written for the foreseeable future after that in that area of the world with the easy oil---the Persian Gulf.

**Q. Hasn't natural gas become the marginal fuel?**

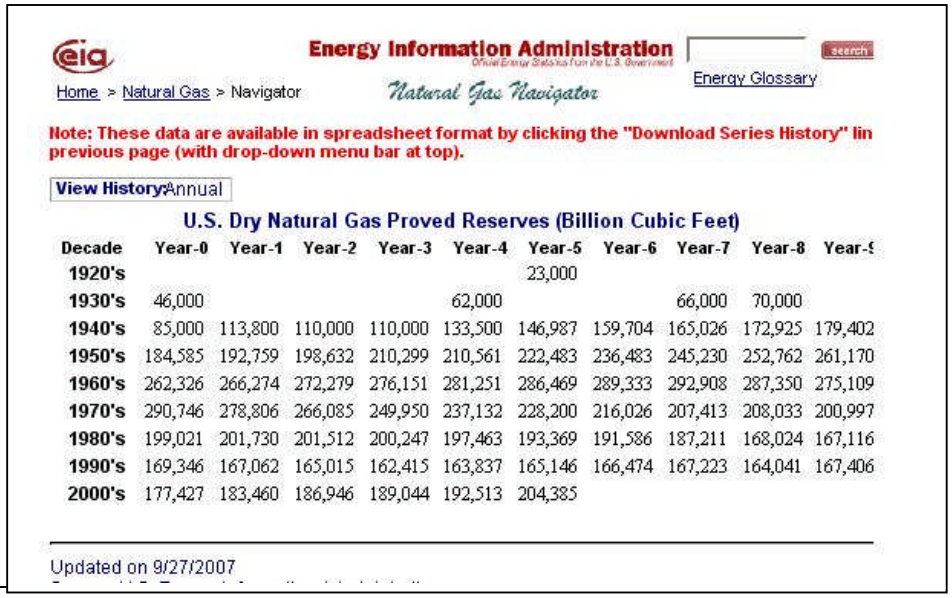
A. Yes, due to this oil dependence, as well as a number of other factors such as environmental drivers and the emergence of the highly efficient combined cycle gas[11] turbines (CCGT), natural gas became the favored fuel of choice in the mid to late 1990's coincident with the drive for deregulation. The cost escalations and talk

[11] In this sense, the word "gas" is understood to mean the working fluid used to drive the turbine rather than to mean "natural gas" but natural gas is a preferred fuel for the CCGT.

of potential shortages were foreseen.[12] In 1997, EES testimony on deregulation to the [then] Connecticut Energy & Public Utilities Committee stated:[13]

> Instructive in this regard was a June 7, 1996 conference at Boston University. At it, Andrew Aitken, a Vice-President of New England Electric System told the audience that in a very short number of years they had gone from 4% natural gas generation to 34%. Growth in natural gas use throughout the nation for electrical generation and for other purposes such as compressed natural gas vehicles (particularly if instabilities continue to grow in the Saudi Arabia) may put pressure on available supply and cost….[14]
>
> …In the long run, a lack of diversity will result in spiraling cost of gas and, Connecticut, as always, on the end of every energy supply line, will pay relatively more than the rest of the nation wiping out many of the gains promised by deregulation and competition.

It took no crystal ball to see supply problems coming; what has been called the "dash to gas" was evident as early as ~1995[15] by some who foresaw the trend. This will lead to another unfortunate trend; increased importation of liquefied natural gas (LNG) to meet still-growing demand. The following table/charts paints the picture for the future.



Energy Information Administration

Official Energy Statistics from the U.S. Government

Search

Home > Natural Gas > Navigator

Natural Gas Navigator

Energy Glossary

Note: These data are available in spreadsheet format by clicking the "Download Series History" lin previous page (with drop-down menu bar at top).

View History: Annual

U.S. Dry Natural Gas Proved Reserves (Billion Cubic Feet)

| Decade | Year-0 | Year-1 | Year-2 | Year-3 | Year-4 | Year-5 | Year-6 | Year-7 | Year-8 | Year-9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1920's | | | | | | 23,000 | | | | |
| 1930's | 46,000 | | | | 62,000 | | | 66,000 | 70,000 | |
| 1940's | 85,000 | 113,800 | 110,000 | 110,000 | 133,500 | 146,987 | 159,704 | 165,026 | 172,925 | 179,402 |
| 1950's | 184,585 | 192,759 | 198,632 | 210,299 | 210,561 | 222,483 | 236,483 | 245,230 | 252,762 | 261,170 |
| 1960's | 262,326 | 266,274 | 272,279 | 276,151 | 281,251 | 286,469 | 289,333 | 292,908 | 287,350 | 275,109 |
| 1970's | 290,746 | 278,806 | 266,085 | 249,950 | 237,132 | 228,200 | 216,026 | 207,413 | 208,033 | 200,997 |
| 1980's | 199,021 | 201,730 | 201,512 | 200,247 | 197,463 | 193,369 | 191,586 | 187,211 | 168,024 | 167,116 |
| 1990's | 169,346 | 167,062 | 165,015 | 162,415 | 163,837 | 165,146 | 166,474 | 167,223 | 164,041 | 167,406 |
| 2000's | 177,427 | 183,460 | 186,946 | 189,044 | 192,513 | 204,385 | | | | |

Updated on 9/27/2007

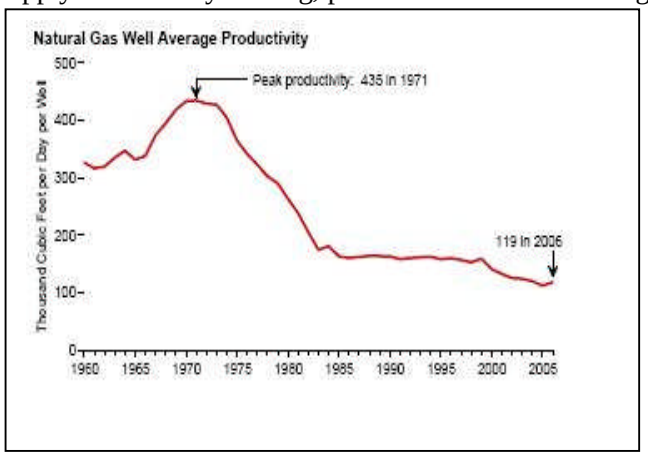
[12] As early as December 1989, when Connecticut suffered at least a week (24th to 31st) of subzero weather, the gas companies and the regional gas association took out full page ads in the Hartford Courant requesting people to conserve. This was at a time when gas for electric generation might be considered negligible.

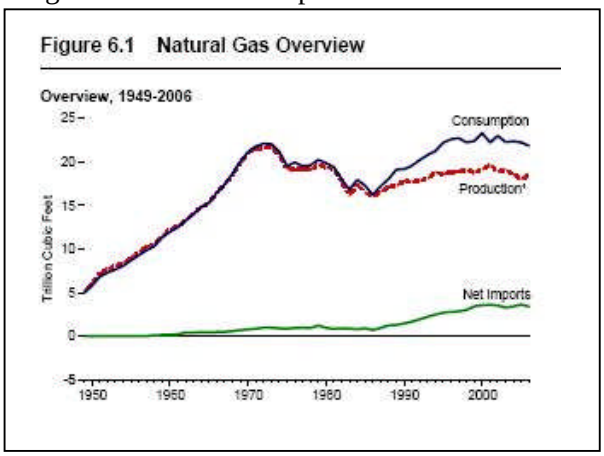
[13] Statement of Joel N. Gordes. Reliability in a Competitive Environment: The Need for Conservation & Load Management and Renewable Energy Sources Under Restructuring. Energy & Technology Committee Public Hearing on HB 6774. February 27, 1997

[14] It is interesting to note that within the last several weeks there have been two additional indicators of further potential pressures on natural gas: 1) T. Boone Pickens has developed a plan (http://www.pickensplan.com/theplan/ ) wherein greater use of natural gas plays a major role(particularly for transportation) as a bridging fuel which would greatly increase it use; and 2) there are discussion between Russia, Iran and Qatar to form a natural gas cartel which, while difficult to develop and maintain, might still negatively impact the price of this fuel.

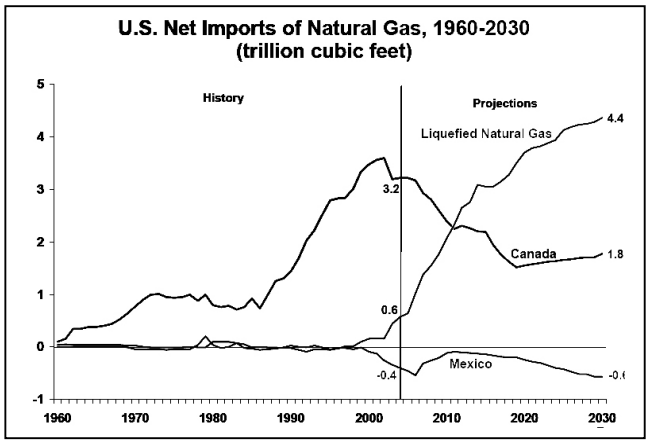
[15] Dr. Carl Weinberg, former Manager of RD&D at PG&E, spoke to this at the 1994 or 1995 NARUC Conference in Madison, WI.

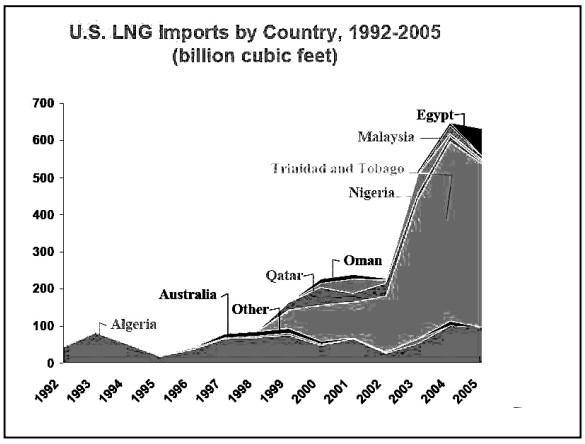
The table on the preceding page shows some of the first increases in proved reserves in some time and beginning in the more recent years. This should be taken in context that we must now provide supply for not only heating, process and hot water but growing amounts of electric power.




While the reserves have increased, the chart to the upper left shows that coincident with that is a further decline in the average productivity per well. The chart at the right shows that in spite of the increase in reserves, there is still a gap between US production and consumption that must be met by imports. As additional gas is required so will the need for imports unless more domestic reserves are available.




The chart at the upper left shows the projected rapid increase in the importation of LNG to make up a portion of the domestic production deficit. The chart to the right depicts what countries will be the most likely nations of origin.

One question becomes "might dependence on this LNG have negative energy security repercussions on the nation and/or the state?" Recalling that the [Kean-Hamilton] 9/11 Commission Report said that event "revealed four kinds of failure: in imagination, policy, capabilities, and management."[16] EES submits the following "imaginative" scenario as an example of how we may wish to begin to think:

[16] *The 9/11 Commission Report* . W.W. Norton & Co. New York. p. 339.

- Proponents of the Broadwater floating LNG facility have emphasized the need for LNG at lower cost without, EES believes, fully balancing that with increased dependence upon potentially risky foreign LNG sources.

- The risk is currently perceived as one with only very localized damage affecting the facility itself and shoreline areas by fouling oyster beds and Long Island Sound.

- Consider a scenario timed 5-10 years hence when regional dependency on this facility and one at the Everett, MA provides ~20% or greater of the NE natural gas supply.

- If terrorists were to simultaneously destroy the two facilities on a sub-zero day such as those in December 1989[17], there is potential for catastrophic human suffering with a potential choice between gas for heating or electricity.

- It could be especially disastrous if they were smart enough (and they are) to wait for an ice storm as in 1973 which turned Connecticut into a skating rink. This would hamper emergency vehicles from moving people to heated shelters.

Preposterous? Remember the "failing of imagination" caution by Kean-Hamilton et al. An entirely different set of LNG security considerations should also be considered:

- The second largest source of foreign LNG is Algeria. Information indicates that it may be a primary source of LNG for Broadwater.

- Algeria was about to have free elections in 1991 but fundamentalists were poised to win that election. That would have been the last free election after Islamic Holy Law would certainly be imposed. One man, one vote, once as Fareek Zakaria intoned.[18]

- The military sprang a coup to prevent that but left another politically fragile situation that has resurfaced in recent years re-emphasizing the risk in dealing for essential commodities in that part of the world.[19]

.

- Surprisingly, the #1 supplier of LNG is Trinidad/Tobago which has its own homegrown fundamentalist group, Jamaat-al Muslimeen, that attempted a coup in 1990.

- More recently a plot to blow up fuel pipelines at JFK Airport in early June 2007 had connections to that same Islamist group based in Trinidad. They are presumed active.

- It is interesting that we may increase exposure to greater dependency on LNG resources that could fall under control of fundamentalist Islam forces by increasing imports. EES does not believe this to be a sound policy, particularly if it necessitates armed intervention.

[17] The gas companies and the regional gas association both ran full page ads on Dec. 24th and 31st in The Courant begging for conservation efforts by consumers. Available on request.
[18] Zakaria, Fareed. The Future of Freedom. W.W.Norton & Co. (New York). 2003.
[19] *Another Brutal Attack in Algeria.* Hassane Meftahi. Associated Press. September 9, 2007.

**Q. Do you have any solutions?**

A. Yes. Despite the appeal of the trend toward lower cost in some aspects of the LNG business over time,[20] the Siting Council may wish to subject new facilities to far more scrutiny on all facets of fuel security than is currently required. As a BMP, the Siting Council could attempt to minimize our dependence on such uncertain sources by promoting as much combined heat and power (CHP) as possible that maximizes efficient use of existing natural gas supply. Possibly including a "public need" for greater efficiency and use of scarce resources. While PA 05-1 and PA 07-242 have made beginnings in this direction, rigorous security review and consideration would provide another powerful driver in this direction particularly if combined with one suggestion for the CSC to consider mandating fuel (not carbon) "offsets" on new facilities over 25 MW. A model for such action was Morro Bay, CA where a moratorium on new home construction was in effect due to a shortage of fresh water. In 1985 the moratorium was rescinded and an offset mechanism enacted that allowed for building a new home if a builder retrofitted ten older homes with water-saving devices.[21] A more local example of offsets involving carbon was the construction of the AES Thames coal plant with concurrent [voluntary] action by developer Roger Sant to plant 52 million trees in Guatemala to offset CO2 emissions.[22] What EES proposes is investigation by the CSC as part of its BMP to have electric plant developers fund retrofits for energy efficiency measures or enhanced boiler/burners on gas-fired schools, hospitals and government facilities to free up additional natural gas. Even retrofits for CHP applications in private sector industrial parks[23] as offsets for new gas-fired central electric plant should be considered. This is a partial solution.[24]

## IV. THE THREAT OF GRID COMPONENTS FOREIGN DEPENDENCY

[20] http://www.eia.doe.gov/oiaf/analysispaper/global/lngindustry.html
[21] "A Gallon Saved is a Gallon Earned." Harrowsmith Magazine. Circa 1985. p. 110.
[22] Meadows, Donella M. "Burning Coal in Connecticut, Planting Trees in Guatemala." Register Citizen. March 27, 1989. p. 13.
[23] The CSC should also be made aware of a CEAB study being performed by the CT Academy of Science and Engineering to determine the feasibility of large-scale CHP on generators over 65 MW. This would also maximize over efficiency if feasible
[24] This might even be undertaken on a build, own operate (BOO) business structure so the developer could also profit from this transaction as well as from their primary project proposal.

**Q. What do you mean by grid components foreign dependency?** [25]

A. Since the 1970's there has been a growing trend toward an increasingly large percentage of major components in the electric grid to no longer be manufactured in part or in whole in this country. The table on the following page[26] provides a snapshot of where the primary global transformer manufacturers are located, what percentages of the North American market they supply and whether they manufacture within the US. In the case of large Generation Step Up (GSU) transformers, many are also approaching their end of life and can take 18-24 months to secure a replacement.

Even if such transformers can be made available there may also be the problem of transporting such heavy, bulky components safely to their point of use. This can be complicated further by the US rail infrastructure that may not be adequate to move such equipment necessitating work-arounds that may not always result in optimal outcomes.

| Company | % of North American market | Manufacturing location | |
|---|---|---|---|
| | | United States | Offshore |
| ABB | 27–29 | Y | Y (Worldwide) |
| Seimens/VA Tech | 22–24 | N | Y(Worldwide) |
| GE-Prolec | 11–13 | N | Y(Mexico) |
| Hyundai | 10–12 | N | Y(Korea) |
| HICO (Hyosung) | <5 | N | Y(Korea) |
| Pauwels | <5 | N | Y(Belgium) |
| Waukesha | <5 | Y | N |
| VTC | <4 | N | Y(Mexico, India) |
| Kuhlman | <3 | N | Y(Mexico) |
| Mitsubishi | <2 | N | Y(Japan) |
| PA Transformer | <2 | Y | N |
| Areva T&D | <1 | N | Y (France) |
| Compton Greaves | See Pauwels | N | Y(India) |

While the Siting Council might not currently have this responsibility, as a Best Management Practice, it may wish to determine the dependence of each existing facility and each applicant for new construction on foreign equipment sources as a condition of construction. A BMP Recovery Measure might insure generators have access to speedy GSU transformer replacements through bilateral or multilateral contracts to share these

[25] Due to contractual/security obligations, this section must be abbreviated to prevent release of information gathered for another project. The material used here, however, is widely available on the internet. If the conflicting project is eventually cleared for general distribution, a copy will be made available.

[26] *Benefits Of Using Mobile Transformers And Mobile Substations For Rapidly Restoring Electrical Service*. US Department of Energy. August 2006. p. 21.

resources with other generators. Other critical components might also be investigated and contracts required in ensuing dockets.

## V. CYBER THREATS TO THE ELECTRIC GRID

**Q: What is cyberwar/cyberterrorism?**

A: An early definition of information warfare was 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.[27, 28]

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

In a more physical form there is electromagnetic pulse (EMP) that can incapacitate any appliance, generator, auto or other device that has incorporated "unhardened" silicon-based semiconductors or chips. This takes place when there is a nuclear blast or via a relatively inexpensive device (~$400) called a flux compression generator is used to induce an EMP similar to what accompanies a nuclear blast.[29] This is a not a particularly high-tech device to build nor does it require a sophisticated aerial delivery system since the device could take on various shapes and be delivered by 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

[27] Winn Schwartau, *Information Warfare, Electronic Civil Defense*, Thunders Mouth Press, New York, 1996. p. 584. Part of this was used previously in discussing the new face of warfare on page 4.

[28] Some accounts add embedded coding in electronics of foreign origin.

[29] Wilson, J. "E- Bomb," Popular Mechanics. 9/2001. pp. 50-53.

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 virtually useless.

Finally, in a lesser known form, a semiconductor-controlled device manufactured in another country might have embedded within its coding for a series of commands that could lead to a parts failure. A CIA document released in 2004 details exactly such an outcome when in 1982 a US valve was purportedly planted for use for a Soviet natural gas line and programmed to fail on command. It is said to have brought about what was said to be the largest non-nuclear explosion ever seen from space.[30] Other variations on this include embedding malware (dangerous coding) in everything from iPods to GPS systems which may be plugged into computers during transfer of data. This can infect a computer or a network if antivirus software is not installed or kept up to date.[31]

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

A: One incident that identified early recognition of vulnerability took place locally and offered insight into the potential repercussions. It took place in downtown Hartford, CT 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."[32]

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 desktop. The Travelers event took place before we became so digitally dependent ---and it took place over a relatively calm weekend. To provide an extremely rough idea of how large

[30] US Caused Soviet Gas Explosion. David Hopffman. HC/Washington Post. February 22, 2004. Some questions on the authenticity of this account have surfaced since then.
[31] Robertson, Jordan. Pre-Installed Viruses: Some Tech Gadgets Come Loaded With Unwanted Extras. Associated Press. March 14, 2008.
[32] Stertz, B. "Crow Short-Circuits Phone, Power," *The Hartford Courant*. 2/20/1983.

business losses could become, the table on the following page supplies the cost per hour of down time for various types of digital businesses:[33]

| Industry | Average Cost of Downtime | Source[34] |
|---|---|---|
| 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 |

**Q.Who else besides yourself has been concerned with these threats?**

A. One person who is concerned and has articulated the threats far better than EES is Lt. Colonel William Flynt (Ph. D., USA-R), a former "Red Team" member with the National Security Agency, who has stated:

> 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.[35]
>
> There is a discussion that sometimes takes place around SCADA[36] 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.[37]
>
> 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…[38]

In describing another exercise he recounted:

---

[33] To be candid, this method of lost capacity, while commonly used, actually provides a grossly distorted picture of potential losses. Sometimes it will overestimate losses while in others underestimates them.

[34] 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.

[35] .Matthew L. Wald, "Electric Power System is Called Vulnerable, and Vigilance is Sought," New York Times. 2/28/02. See http://www.box.net/shared/2h5b7zy9g5 for ISO NE/NY cyber conference. A portion of this was used previously at p.4.

[36] SCADA refers to Supervisory Control and Data Acquisition Systems used to control and provide information on many aspects of power system operations.

[37] William Flynt, Ph.D., *Terrorism and the Electric Power Infrastructure*, Keynote Session, International Conference on Advanced Technologies for Homeland Security, UCONN, September 25, 2003.

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

> 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.[39]

The US-Canada Power System Task Force's (blackout) draft report, in one of its more informative portions (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.[40]

There are numerous other concerned persons mentioned in my 2004 Statement of Limited Appearance in CSC Docket #272 who share these opinions to one degree or another. This may be accessed at http://www.ct.gov/csc/lib/csc/jgordesltdappear.pdf

More recently[41] CNN featured an experiment at the Idaho National Laboratory which has been deeply involved in cybersecurity issues for a number of years. They released a video of an exercise where they destroyed a generator by hacking into its control system. Presumably they were able to remotely change the generator frequency which led to its destruction. (See video at:

http://www.cnn.com/2007/US/09/26/power.at.risk/index.html#cnnSTCVideo )

In January 2008, the CIA called a news conference to alert the public that several foreign electric utilities had been hacked. A Washington Post story noted:[42]

> In a rare public warning to the power and utility industry, a CIA analyst this week said cyber attackers have hacked into the computer systems of utility companies outside the United States and made demands, in at least one case causing a power outage that affected multiple cities.
>
> "We do not know who executed these attacks or why, but all involved intrusions through the Internet," Tom Donahue, the CIA's top cybersecurity analyst, said Wednesday at a trade conference in New Orleans...

[39] William Flynt, Ph.D. Op cit
[40] US-Canada Power System Outage Task Force: Causes of the August 14th Blackout. pp. 94 & 99.
[41] September 27, 2007.
[42] Nakashima, Ellen and Mufson, Steven. *Hackers Have Attacked Foreign Utilities, CIA Analyst Says*. Washinton Post. January 19, 2008. p. A04. Full article available at http://www.box.net/shared/khjqd5pa4m

> …Over the past 10 years, electric utilities, pipelines, railroads and oil companies have used remotely controlled and monitored valves, switches and other mechanisms. This has resulted in substantial savings in man power and other costs...
>
> …The U.S. electricity grid has always been vulnerable to outages. "Cybersecurity is a different kind of threat, however," Joseph T. Kelliher, the commission's chairman, said in a statement this week. "This threat is a conscious threat posed by a single hacker, or even an organized group that may be deliberately trying to disrupt the grid."

## VI. MORE DISTRIBUTED GENERATION & GRID DECENTRALIZATION MAY LESSEN VULNERABILITY.

**Q. What is your definition of distributed generation?**

A: Because of questionable statements made before the CT DPUC and the Energy & Technology Committee by the ISO-NE and one utility in a previous proceeding (DPUC docket #02-04-23), EES stresses the criticality of defining distributed generation. EES has provided a composite definition derived from such diverse and credible groups as the US DOE (2 definitions), Electric Power Research Institute (2 definitions), American Gas Association (1 definition) and the California Energy Commission (1 definition).[43] A composite of their definitions might read:

> Distributed resources include conservation and load management with modular electric generation and/or storage located near the point of use either on the demand or supply side. DR includes fuel-diverse fossil and renewable energy generation and can either be grid-connected or operate independently. Distributed resources typically range from under a kilowatt up to 50 MW. In conjunction with traditional grid power, DR is capable of high reliability (99.9999%) and high power quality required by a digital society.[44]

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

A: There are numerous attributes in the many technologies that make up what is called "distributed generation" that can make it attractive security-wise but also to business and industry as well as grid planners and owners. These include but are not limited to:[45]

**Reliability.** One of the major advantages of distributed generation is its ability, in conjunction with grid-supplied power, to provide reliability in the 99.9999% range required by many businesses who are now dependent upon digital technologies.

**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 and require hours or days lost in having to reacquire data or in reprogramming.

---

[43] Full definitions from these sources are available at: http://www.box.net/shared/khjqd5pa4m. Actually, EES dislikes this composite definition but the sources for it are citeable.

[44] Please note the author is aware of the definition of distributed generation in PA 05-1, AAC Energy Independence, as being set to 65 MW. This is outside the norm for published figures by others.

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

**Modularity.** 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 endeavors.

**Deferral of Transmission and Distribution Costs.** In some situations, distributed technologies may offer a lower cost option than traditional transmission and distribution upgrades such as substations or new high voltage lines. At some point this may be a lower cost option when those in the private sector elect to install DG on the customer side of the meter for power reliability/quality reasons. It may also be in conjunction with resources on the utility side of the meter as well..

**Reduced System Losses**. There is less line loss with generation closer to points of use.

**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 had been the situation of three TM-2500 units that had supplied 69 MW of power for use during summers in the SW CT load pocket.

**Lower Operations and Maintenance (O&M) Costs**. Some DG units have low O&M costs.

**Lower Financial Risk**. There is less financial risk with small-scale projects than with large ones. Lenders face a lower risk in investment into numerous but small, diverse distributed projects.

**Less Regulatory Risk**. There is less risk of regulatory changes for the short planning and installation cycle of a distributive technology as opposed to larger plants.

**Lower Fuel Diversity Risk**. Since many of these new technologies can use multiple fuels or renewable energy sources there is fuel risk reduction.

**Ease of Siting.** It has become increasingly difficult to locate large generation and transmission facilities and the siting process can take many months if not years if oppositions arises.

**Short Lead Times**. Shorter lead times mean fewer financial uncertainties. Since distributed technologies are manufactured in the factory rather than constructed on-site, there are fewer risks associated with lead times. Economies of scope can also be realized.

**Incentives from Deregulation**. Deregulation 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 deployment. The Renewable portfolio Standard also can add value for these technologies as can new values from the Regional Greenhouse Gas Initiative.

**Environmental Improvement**. Many distributive technologies result in low emissions of criteria pollutants. They also generally produce lower greenhouse gas emissions than traditional electric generation. This can also result in a shortened regulatory review process.

Despite these advantages, in cyberwar, redundancy, alone, as represented by distributed generation, is not enough to provide resiliency, it must also be decentralized, another grossly misunderstood term. For example, the A-7 Corsair II fighter aircraft has a duel hydraulic control systems (redundancy) but because both hydraulic lines are in close

proximity to each other in certain critical areas, there is a high likeliness that antiaircraft ordinance can disable both systems simultaneously.[46,47] While it is "redundant" it is not adequately "decentralized" and still vulnerable in this analogy.

Lovins and Lovins define decentralization (in terms of physical vulnerability but is mostly applicable to cyber) as having the following attributes: [48,49]

- **Unit scale**. "Scale" in this sense means the smaller size or output capacity of a single unit of supply than usually found in centralized systems as a percentage of total power.

- **Dispersion**. Refers to whether units are concentrated or distributed, *relative to each othe*r.

- **Interconnectedness**. Separate units can be coupled to each other, stand-alone (connected only to the end-user), or both optionally so as to isolate failures and permit autonomy when needed. Interconnection may increase overall reliability in many cases.

- **Composition**. Different units can be *monolithic* (consisting of inseparable parts) or *modular* (combining multiple sub-units). Gas turbines, fuel cells & photovoltaic arrays are modular; central thermal plants are more monolithic.

- **Locality** -the heart of *"decentralizatio*n," wherein *local* units are near end users, linked by short supply lines to reduce vulnerability. Oddly, most wind energy is not decentralized DG.

- **User-controllability**. Ability to choose/control the energy systems and whether they are participatory and pluralistic or dominated by a central technical elite.

- **Comprehensibility**. The ability to control a technology depends partly on whether they can understand it. A system can be understandable even when technically very sophisticated.

- It is important to remember, even in a specific context, that all the dimensions of "decentralization" are relative, not absolute.

## VII. A SIX POINT CYBER-DEFENSE STRATEGY

**Q: Do you have any further suggestions on what we may need in terms of security for the CSC Best Management Practices?**

A: Yes, I do. I suggest the following points be considered for inclusion in the BMPs:

[46] Discussion with John Millar, a former Naval Aviator on 8/23/03.

[47] Decentralization principles in warfare are ancient. In Leo Tolstoy's fictional *War and Piece* (1865/1869) the character Prince Andrei Bolkonsky cautioned his troops "'M. l'aide-de-camp,' he shouted, 'tell the men not to crowd together.'" p. 756 Flare Books, 1973 edition.

[48] Lovins, Amory B. and Lovins, L. Hunter, Brittle Power, Energy Strategy for National Security, Brick House Publishing Co. (Andover, MA) 1982. P. 218. This book was originally a study conducted for the Pentagon's Defense Civil Preparedness Agency.

[49] Another more recent book on decentralization worth investigation by CSC for BMPs is The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations. [2006. Penguin Group.] by Ori Brafman and Rod A. Beckstrom. It provides a fascinating account of how decentralized organizations have greater resiliency. Please also note that as of March 20, 2008, Mr. Beckstrom has headed the National Cyber Security Center of the Department of Homeland Security (DHS).

1) Large new transmission line plans by utilities to alleviate power congestion may further centralize electric power and actually invite vulnerability to cyber and physical attacks. The National Research Council (National Academies of Science, Engineering, etc.) has stated in regards to adding transmission lines for congestion relief:

> A direct way to address vulnerable transmission bottlenecks and make the grid more robust is to build additional transmission capacity, but there are indications that redundancy has a dark side (in addition to increased costs). The likelihood of hidden failures in any large-scale system increases as the number of components increases. Modeling techniques are only now emerging for the analysis of such hidden failures." (see, for example, Wang and Thorp, 2001).[50]

New transmission projects or alternatives to them should also be planned to consider implementation of smart grid/intelligent grid/adaptive grid technologies that allow separation of affected areas into microgrids or minigrids. The existing grid should eventually also be retrofitted in the same manner. Further deployment of technologies such as autoreclosers, sectionalizers and even "smarter" follow-ons to these may be useful early steps. Public Act 07-242, Sections 21-36, dealing with Energy Improvement Districts, may also be useful in becoming a model for this. The Electric Power Research Institute (EPRI) appears to support moving in this direction when it stated:

> A portfolio of innovative technologies…. can comprehensively resolve the vulnerability of today's power supply …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…[51]

But EPRI also goes on to observe the reality that:

> 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... Capital expenditures as a percent of revenue are at an all-time low... There is little incentive for introducing new technology…

CSC, through its siting powers alone, may not be able to force movement in this direction without coordination and cooperation with the DPUC, OCC and other agencies. The DPUC's ability, however, to exercise Decoupling/Performance-Based Ratemaking with utilities can not only drive <u>but adequately reward</u> utilities for new technology deployment which may be the more palatable solution for all involved.

---

[50] *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism. National Academy Press. Committee on Science and Technology for Countering Terrorism, National Research Council. p.302.* 2002.

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

2) Use of energy efficiency and load management first, followed by small, fuel diverse generators that are close to loads but adequately dispersed may provide a more robust system that is less vulnerable to physical and cyber attacks. These should be considered as primary steps before further large transmission projects are instituted. PA 07-242 does call for all cost-effective demand side resources to be considered before generation and the CT Siting Council might take note of that when looking at new transmission projects as well.[52]

3) The CSC should also consider that some Connecticut firms produce distributed generators such as fuel cells, gas turbines, turbine components, and even photovoltaic components[53]. This could provide a major economic boost to the state's economy if implemented in the proper way.

4) The CSC should consider that distributed generators would be largely paid for by businesses and placed on their premises to run with the grid as a back-up to insure power reliability and quality. As such, the cost may be less than transmission lines for which ratepayers would foot (subsidize) the entire bill.

5) Because much DG is clean and modular, distributed generation options for congestion alleviation, under a favorable CSC and DPUC regulatory scheme, may be quicker to implement than power lines due to less regulatory delays and legal challenges.

6) Another suggestion, but not under CSC auspices yet, is to allow some DG project involvement by the utilities who would then be able to ratebase their contributions to projects up to 25-50 megawatts.[54] This would provide utilities an incentive not to oppose alternatives that are in the interests of security yet earn a comparable rate of return or better if a management fee of 1% to 8% based on performance is allowed for such activities as it currently is for C&LM efforts. Favorable regulatory treatment for

[52] Actually, point (9) of 16a-35k, The Connecticut Energy Policy Act, essentially said the same thing beginning in 1992 but possibly is more specific to generation.
[53] STR of Enfield , CT supplies encapsulant material for many PV manufacturers.
[54] The Hartford Courant article "Profits Up 45% at NU for Quarter" 11/11/08, p.16 recounts this increase was due to the company being "heavily invested in high-voltage transmission projects." The risk in this is if this is the primary means of increasing earnings, projects may be proposed that may not be necessary and could conceivably merely add additional points of failure as per the National Research Council's warning at page 20 and footnote 47. Providing other means to earn a return may mitigate such proposals.

DG/CHP would take a page from the Netherlands that allows utilities to build CHP facilities in that nation and has resulted in 40% of their power supplied in that manner.[55]

In addition, the National Science Council's previously cited study has made the recommendation that use of homeland security funds for funding distributed generation to maintain critical 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.[56]

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. [57]

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

Finally, EES suggests the CSC (and others) investigate the metrics in the paper "Rating the States for Energy Security" presented at several conferences and available at: http://www.dsireusa.org/documents/PolicyPublications/Rating_the_States_ASES_2003.pdf This paper uses Connecticut as an example (last pages) and, at its writing in 2003, the state scored 45 out of 100 points. While in need of a drastic update, EES suspects the score would be substantially higher today, but, still, it provides for CSC some considerations in setting BMPs.

## VIII. CLOSING STATEMENT

**Q: Do you have a closing statement?**

---

[55] James Lucky, *Distributed Power Dutch Style*, Energy Markets, June 2001, p. 8.
[56] *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.
[57] Electricity Sector Framework for The Future, Volume I, Achieving A 21st Century Transformation. Electric Power Research Institute. August 6, 2003. p. 7.

A: Yes. A Best Management Practice for the CSC on grid security should not look at the siting of each component in isolation. A BMP needs to determine what the effect of each new addition to the grid does in relation to the whole -- holism. As noted earlier, remarks by the National Science Council note that merely adding transmission without regard to its security considerations can perversely add additional points of failure thereby jeopardizing reliability, resilience and security.

Additionally, indications suggest preparation to meet multiple threats to the grid must be addressed by public/private partnerships from planning, construction, continuing maintenance and improvement to a more resilient system. CSC can play a vital public role by development of BMPs that address not only the more conventional threats but those newly emerging ones that may be the measure of conflict in the 21st century.

Existing and well-proven, as well as new technologies, can provide this more resilient "smart grid". Construction of only large transmission facilities has the potential to lock us into an electric Maginot Line for decades. In retrospect, solely building lines without incorporating enhanced resilience may be looked upon in the future as imprudent at best and negligence at worst leaving all parties open to future litigation . With simple and relatively inexpensive steps this may even present profit centers for utilities, private sector developers, Connecticut-based businesses and future litigation may be avoided. The Siting Council may wish to heed the EPRI's advice:

> 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.[58]

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