Energy Security

By
Matthew H. Brown
Christie Rewey
Troy Gagliano

National Conference *of* State Legislatures

The Forum for America's Ideas

William T. Pound
Executive Director

7700 East First Place
Denver, Colorado 80230
(303) 364-7700

444 North Capitol Street, N.W.
Washington, D.C. 20001
(202) 624-5400

April 2003

The National Conference of State Legislatures is the bipartisan organization that serves the legislators and staffs of the states, commonwealths and territories.

NCSL provides research, technical assistance and opportunities for policymakers to exchange ideas on the most pressing state issues and is an effective and respected advocate for the interests of the states in the American federal system.

NCSL has three objectives:

- To improve the quality and effectiveness of state legislatures.
- To promote policy innovation and communication among state legislatures.
- To ensure state legislatures a strong, cohesive voice in the federal system.

The Conference operates from offices in Denver, Colorado, and Washington, D.C.

Printed on recycled paper

ISBN 1-58024-287-1

Contents

List of Figures and Tables

Figure

Table

About the Authors

NCSL is a nonprofit, bipartisan organization that works to improve the quality and effectiveness of the nation's 50 state legislatures. NCSL's Energy Program assists state legislatures on a variety of energy issues including electric industry restructuring, utility taxation, energy efficiency and renewable energy.

Matthew H. Brown is the director of the National Conference of State Legislatures' Energy Project. He is responsible for advising state legislators on a wide variety of energy issues. Mr. Brown has authored or co-authored numerous publications on electric industry issues. He has testified before more than 30 state legislative bodies on electric industry issues, and worked closely with many state legislatures on their own electricity policies. Mr. Brown holds an MBA.

Christina M. Rewey is a policy associate in the Energy Program at NCSL. Ms. Rewey provides support to state legislatures on a variety of energy issues. Ms. Rewey holds a bachelors' degree in political science with a minor in environmental issues and is currently enrolled in a master's in public administration program.

Troy Gagliano is a policy specialist in the Energy Program at NCSL. Mr. Gagliano testifies before legislative committees, provides technical and research assistance to legislators and staff, and publishes reports and articles on a various energy-related topics. He holds a master's degree in international public policy.

Acknowledgments

This report was prepared with the financial support of a grant from the U.S. Department of Energy (DOE) Office of Energy Assurance, Denise Swink, director. Christian Ford, formerly of that program, provided helpful input and review.

The authors are grateful for the assistance of numerous others who assisted in providing information for this report and its review. Bill Becker of the Department of Energy, Greg Dana of the Alliance of Automobile Manufacturers, Kansas Representative Carl Holmes, Tim Kichline of the Edison Electric Institute, David Lovell of the Wisconsin Legislative Council, Maryland Delegate Carol Petzold, Jack Rigg of BP America, Terry Ross of the Center for Energy and Economic Development, and Samantha Slater of the Electric Power Supply Association provided reviews and also are members of the NCSL Advisory Council on Energy (ACE), an advisory board to the NCSL Energy Project.

The authors also thank Jeff Pillon of the Michigan Public Service Commission, Charles Davis of the University of Missouri's FOIA Center, Larry Brown of the Edison Electric Institute, Landis Kannberg of Pacific Northwest National Labs, Mike Hyland of the Public Power Association, and Mark Bennett of the Electric Power Supply Association. Jim Reed of NCSL assisted with the section on nuclear fuel transportation and Cheryl Runyon on a number of other nuclear power issues. Leann Stelzer of NCSL edited the report. Finally, Scott Liddell of NCSL formatted the report for publication.

Executive Summary

The nation's energy system is a complex, interconnected web in which a disruption in one part of the infrastructure can easily cause disruptions elsewhere in the system. After September 11, 2001, many policymakers and industry experts focused increased attention on the system's vulnerability to intentional attack, accident or natural disaster. Now, energy security has become an important consideration for state legislatures.

The following are some particular aspects of the system infrastructure that remain vulnerable:

The electricity system

- Nuclear facilities
- Non-nuclear power plants
- Nuclear fuel storage and transportation
- Electric transmission lines
- Electrical substations

The natural gas system

- Natural gas storage facilities
- Natural gas pipelines

Petroleum

- Crude oil storage and transport
- Fuel oil
- Refineries
- Petroleum product pipelines and terminals, including marine terminals
- Cyber security
- Telecommunications systems

The federal government plays a significant role in protecting these sectors of the energy industry and in preventing and managing energy crises. Major federal agencies and their responsibilities include:

- **Department of Homeland Security (DHS)**: The DHS role is to prevent terrorist attacks within the United States, reduce the nation's vulnerability to terrorism, minimize damage and assist in the recovery from terrorist attacks, perform emergency planning for natural and manmade crises, and ensure that homeland security efforts do not diminish overall economic security. The Information Analysis and Infrastructure Protection Division will analyze infrastructure needs and set priorities for security measures. DHS will focus on vulnerable targets with catastrophic potential, such as nuclear power plants, chemical facilities, pipelines and ports. The agency then will establish policy for standardized, tiered protective measures that address the perceived threats.

- **Federal Energy Regulatory Commission (FERC)**: Monitors and regulates the nation's electric industry. FERC approves rates for security-related measures at power plants or in power lines, especially for merchant power plants. FERC also regulates key energy facilities such as siting of interstate natural gas pipelines as well as the safety of hydro dams.

- **Nuclear Regulatory Commission (NRC)**: Has jurisdiction over nuclear power generation, waste, and storage issues.

- The Commerce Department **Office of Pipeline Safety** is involved in pipeline safety regulation; the Department of Homeland Security's **Transportation Safety Administration** (TSA) is beginning to assert regulatory authority over pipelines, although just how the TSA will regulate and coordinate with the Office of Pipeline Safety is yet to be determined.

State governments play a critical role in effectively preventing and responding to energy security threats. Policy options that states can use to protect themselves fall into two broad categories—prevention and planning, and response. States can determine their vulnerabilities and bolster their energy security through the following policies.

- Freedom of information (FOIA) issues
- Paying for energy security
- Emergency management and response
- Regional energy policies
- Cyber-security issues in energy
- Energy system diversity and redundancy
- Distributed energy
- Energy efficiency and responsive demand for electricity
- Energy facility siting
- Energy/environmental policies
- Energy/transportation policies

NCSL has developed the following list of recommendations and options for state legislatures regarding energy security.

Energy Security Recommendations and Options for State Legislatures

- ✔ ***Seek information and education*** about energy systems and energy security. Through this process, identify vulnerabilities in the energy system.

- ✔ ***Provide for sharing of information and coordinating responses*** between federal, state and local government agencies as well as the energy industry.

- ✔ ***Review utility commission enabling statutes.***
  - ✦ Determine if the state utility commission has sufficient authority to collect information on security from regulated entities and to oversee and approve utility security plans where deemed necessary.
  - ✦ Determine the sufficiency of FOIA exemptions for data submitted to the utility commission regarding the security of critical infrastructure.
  - ✦ Determine if the utility commission has sufficient guidance, authority and oversight related to pass-throughs of security related costs.
  - ✦ Determine if the commission has sufficient guidance related to disclosure of such costs on consumers' bills.

- ✔ ***Identify opportunities for energy efficiency*** and ***encourage demand response*** programs

- ✔ ***Examine*** the security implications of ***state siting laws.***

- ✔ ***Analyze statutes governing the state energy office*** and its duties.
  - ✦ Determine if the state energy office has sufficient authority and budget to:
    - ✘ Provide technical assistance to policymakers on energy security.
    - ✘ Manage state and federal grants that strengthen energy security.
    - ✘ Oversee energy emergency management function.
    - ✘ Oversee an energy analysis and planning function.
  - ✦ Determine how to integrate the state homeland security office with the state energy office

- ✔ ***Study*** statutes to determine the ***diversity and redundancy*** of the energy system. Focus on the potential role of ***renewable energy*** and ***distributed generation*** in bringing this diversity, thereby creating a more secure energy system.

- ✔ ***Review statutes governing freedom of information laws*** (FOIA).

- ✔ Reassess laws and procedures governing ***open meetings***.

- ✔ Evaluate ***state liability statutes***.

- ✔ Ensure that industry and state agencies have conducted appropriate ***vulnerability studies***.

- ✔ Update statutes governing ***emergency response***.

- ✔ Examine legislation regarding ***"unfair pricing" in emergencies***.

INTRODUCTION

The September 11, 2001, attacks on New York and Washington, D.C., forced the nation's energy business and the policy bodies that oversee the nation's energy establishment to reassess many old assumptions. For the first time, a relatively small number of people who had concerned themselves with securing the nation's energy infrastructure were thrust into prominence. Energy security had entered the lexicon of all those involved in the energy industry. Soon after, policymakers, state energy officials, public utility commissioners and emergency management and law enforcement officials discovered a renewed drive to cooperate with electric, gas and petroleum companies to improve the security of systems that generate, transmit and distribute energy.

Energy security affects all facets of the energy policy environment; therefore it is important for individuals and policymakers who focus on seemingly unrelated aspects of energy policy to also understand the overlapping dimensions of these issues.

- Energy security affects utility commissions and rate regulation because the commissions will have to decide whether the utility or its customers will pay for a increasing energy security investments. It also affects the many local governments that operate municipal utilities that might be in need of security investments.

- Funding for research and development may be shifted to support investments that bolster energy security.

- Policymakers also may need to develop plans that address potential conflicts between simultaneously complying with environmental regulations and restoring power during a crisis.

- Energy security affects freedom of information policy, since the United States has had a long tradition of providing a great deal of information to as many people as desire it. Protecting vulnerable infrastructure also may involve reassessing what information to make public under what circumstances.

- Energy security involves economic development and the economic health of the United States. Terrorists have demonstrated through actions and words their intent to damage the U.S. economy. The health of the U.S. economy is intimately linked with energy resources and assets such as power plants, power lines and fuel pipelines, and fuel processing and storage centers. These assets comprise a large portion of the nation's critical infrastructure, and any disruption to these assets could adversely affect the economy.

- Finally, energy security affects numerous other broad energy policy debates and concerns, such as the state energy planning process or state energy emergency plans.

The threat to the U.S. energy system cannot be taken lightly. Critical points within the energy infrastructure—such as electricity distribution networks, gas transportation and storage facilities, or certain power plants—could give terrorists an opportunity to cause catastrophic damage to the economy and to the health and safety of people. The combination of today's current level of security with an already vulnerable energy infrastructure makes energy security one of the highest national and state policy priorities. Energy resources are increasingly complex, interconnected and vulnerable. Owners and operators of energy assets and the federal, state and local policymakers who oversee those assets are generally ill-prepared for a large-scale terrorist attack, although they are currently better prepared than before September 2001.

This primer is designed for state policymakers. It describes the threats to the nation's energy system, it defines local, state and federal roles in preventing and responding to energy security emergencies, and it identifies specific policies that state policymakers can use to address those threats. The primary message of this primer is twofold: 1) the interdependent energy systems of the United States and the rest of North America exhibit vulnerabilities, and 2) state policymakers serve a critical role, in

partnership with industry and local and federal officials, in addressing those vulnerabilities.

The remainder of this document is divided into two major sections. The first section provides a background on energy security and includes a discussion of the vulnerabilities in the energy system. The second section lays out state policy options to address energy security and discusses federal and state jurisdiction as well as action items for state policymakers.

Part I

Background on Energy Security

1. A Definition of Energy Security

Energy security refers to a resilient energy system. This resilient system would be capable of withstanding threats through a combination of active, direct security measures—such as surveillance and guards—and passive or more indirect measures-such as redundancy, duplication of critical equipment, diversity in fuel, other sources of energy, and reliance on less vulnerable infrastructure. The Kansas Energy Security Act defines security as " … measures that protect against criminal acts intended to intimidate or coerce the civilian population, influence government policy by intimidation or coercion or to affect the operation of government by disruption of public services, mass destruction, assassination or kidnapping." Traditionally the focus of energy security has been on accidents and natural disasters. After September 11, 2001, policymakers and industry have had to consider the threat of intentional damage to a much greater degree than before.

Energy security focuses on critical infrastructure; a term that is receiving increasing attention. The Homeland Security Act of 2002 and the USA Patriot Act define critical infrastructure as "systems and assets ... so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (Public Law 107-56(e)). Some of these systems include food, water, agriculture, health and emergency services, energy (electrical, gas and oil, dams), transportation (air, road, rail, ports, waterways), information and telecommunications, banking and finance, postal and shipping, and national monuments and icons. This report focuses on the energy sector's critical infrastructure.

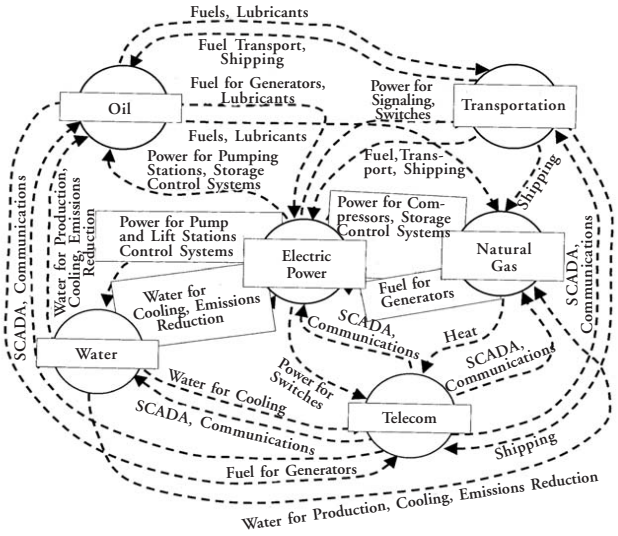
2. The Importance of Energy Security

Energy security matters to state policymakers because of the effect that a security breach could have on the economy, public health and safety, and the environment. The data illustrate the linkage between the country's energy system and these other areas are stark and worthy of attention. They show how central the energy system has become to American citizens' way of life. The energy system has evolved into one piece of a complex web of the nation's infrastructure. Figure 1 illustrates just how intertwined the nation's energy, water, electronics and telecommunications systems are. For example, water pumps rely on electricity to operate. Electricity relies on compressed gas as a fuel, which in turn often relies on electricity to run the compressors. Telecommunications systems serve as a vital support system for the power grid and they too require electricity.

Economic Disruptions

The nation's new high-tech economy demands a reliable, petroleum- and electricity-based energy system to meet its needs. Disruptions in the manufacturing, distribution and marketing of petroleum-based fuels (including jet fuel, diesel, gasoline, fuel oil and natural gas) could also affect the viability of the transportation system. Further, unstable prices that are so low they discourage new investment in energy infrastructure or so high they disrupt the economy can be problematic.

Figure 1. Interrelationship of Energy and Other Critical Infrastructure



Source: Jim Peerenboom, Argonne National Laboratory, 2002.

Data from the California and western power grid energy crisis in 2000-2001 demonstrates just how severely short disruptions in the supply of electricity can affect an economy. Some businesses lost millions of dollars as a result of power outages. A study produced by the Electric Power Research Institute (EPRI) attempted to quantify the costs of power outages.

The EPRI study classified power outages into several categories, some of which lasted for as little as one second, some for three minutes, and others for an hour or more. The study concluded that an outage of any length—even one second—could create a substantial economic loss for many businesses. The losses fall into several categories that include:

- Data losses at computer-based businesses,
- A workforce that is being paid but is unable to work because of the outage,

- Materials loss or spillage (some restaurants or food processing centers are required to dispose of any food that has not been refrigerated for a certain length of time),

- Loss of unfinished products at electronics manufacturing facilities (even very brief outages, less than one second, can cause substantial losses),

- Equipment damage,

- Costs of running backup generation, or

- Costs of restarting equipment.[1]

The study did not attempt to incorporate the effects of a terrorist attack on the nation's infrastructure but, instead, looked at the effect of outages happening today in the electric industry. A focused attack on the electricity system could only be assumed to produce even greater impacts than those projected in this study.

Energy security also has important ramifications for public health and safety as well as the environment.

Public Health and Safety

A major disruption to the nation's energy system would not only interrupt power flows, but also would affect public health. Some of the public health and safety effects of such an event are described below.

- Depending upon its nature, an energy infrastructure attack in an urban area could expose from hundreds to hundreds of thousands of people to serious harm from events such as radiation, toxic clouds, and massive fires.

- The publicly available worst-case scenarios for a variety of refineries discuss serious health effects from huge releases of anhydrous ammonia. (Anhydrous ammonia is explosive when mixed with air and can severely burn the skin, eyes and respiratory tract.) Releases of anhydrous ammonia would threaten surrounding areas, including civil-

ian populations, schools, shopping centers, hospitals and wildlife areas.

- Dams afford an opportunity for terrorists to disrupt power generation. They also expose downstream populations to the risk of harm from the accompanying water surge.

- A significant radiation event from a nuclear plant could affect populations within a 50-mile radius.

- Interruptions in power flows to hospitals or other public infrastructure such as water or sewer systems could pose tremendous challenges. All such systems rely on electricity for vital functions including lighting, refrigeration, monitoring other machinery, as well as pumping and other related functions. This difficulty is mitigated to some degree by the fact that many hospitals and public facilities have available back-up power generation equipment.

Potential Environmental Effects of Energy Security Disruptions

An energy security disruption affects not only human health but also the quality of the environment. A disruption could result in a variety of environmental effects.

- State laws often do not take terrorism into account. Under Texas state law, maritime tanker operators that carry more than 10,000 gallons of oil must have vessel response plans and must take certain steps to limit the potential environmental harms of an oil spill. However, none of these requirements-neither those pertaining to prevention nor to mitigation-deal directly with the special threat of terrorism.

- In a situation where security is breached at a nuclear facility and a radiation release occurs, the potential disruption could render a significant area surrounding the nuclear facility uninhabitable.

- Disruptions—whether from terrorism or from natural disasters—to major power plants or to transmission lines could force the electric system to rely on other less efficient, greater emitting power plants.

- An attack on a well or wells off the Gulf Coast could produce a fairly significant spill that would bring extensive harm to the shorelines.

- A large, full oil tanker carries upwards of 38 million gallons of crude. If such a vessel suffered a terrorist attack large enough to cause the loss of the bulk of its cargo, the environmental effects would be devastating. (By way of comparison, the *Exxon-Valdez* spill is estimated at 11 million gallons.)

3. Vulnerabilities in the Energy System

The energy system in North America is tightly interconnected, both geographically and through the fuels and resources used to power it. Many types of energy facilities are linked and vulnerable in this large, dispersed energy system. The primary types of energy facilities include:

The electricity system

- Nuclear facilities
- Non-nuclear power plants
- Nuclear fuel storage and transportation
- Electric transmission lines
- Electrical substations

The natural gas system

- Natural gas storage facilities
- Natural gas pipelines

Petroleum

- Crude oil storage and transport
- Fuel oil
- Refineries
- Petroleum product pipelines and terminals, including marine terminals
- Cyber security
- Telecommunications systems

The vital importance of these elements of the energy system make them critical to the nation's integrated energy system. Threats and disruptions to one part of the system affect another. For example, a disruption to a natural gas pipeline affects not only the companies and homeowners that use gas for heating, cooking or industrial process, but also the large number of new power plants that use gas to generate electricity. An oil refinery that produces gasoline, jet fuel or diesel fuel may also produce fuel oil for use in power plants. In addition, the refinery may rely on natural gas as its source of power. Hawaii provides an example. Power

plants there use fuel oil that local refineries produce to make electricity. The same refineries that make the fuel oil also produce jet fuel, gasoline, diesel and other products. A disruption to a single crude oil tanker could affect not only the gasoline markets but also the power system in Hawaii, for instance, which relies on oil to power almost all of its power plants. The remainder of this section addresses these vulnerabilities in more detail.

Electricity System

The nation's power plants and transmission and distribution systems are among the more critical facilities in question. Each part of the electricity system has different characteristics and should be seen on its own merits as either vulnerable and worthy of special attention, or perhaps vulnerable but not of either significant threat to public health or to the health of the electric system.

Nuclear Facilities

The nation's 103 nuclear power plants received a great deal of attention even before September 2001, and continue to be a major part of discussions about energy security. Many people assert that the danger from an attack on a nuclear power plant poses both an economic security risk and a public health risk. Others point to the fact—largely because the plants have received so much attention—that nuclear power plants are among the best protected of any of the nation's civilian infrastructure.

Both industry and government have reviewed and increased security measures at these plants. Patriot missiles have been deployed at the Palo Verde nuclear facility in Arizona, and national guard troops are stationed around numerous nuclear facilities, including the Connecticut Yankee and Millstone plants in New England. Industry, in collaboration with government, also performs mock raids on nuclear facilities to test security procedures. Since September 2001, the industry has spent an additional $370 million in security related improvements. By 2003, security expenditures are expected to increase to $7.3 million per site.[1]

Federal policymakers, with input from a host of stakeholders including state government, must determine if these investments are adequate on

an ongoing basis. The purpose of this primer is not to judge whether or not these facilities are secure, but to provide information on security issues and responsibility for addressing those security issues. In general, the federal Nuclear Regulatory Commission oversees all safety issues related to nuclear power plants. State and local government can and do have input into NRC hearings and decisions, much like any other intervenor.

The federal Nuclear Regulatory Commission (NRC) requires, as a condition of obtaining an operating license, that a nuclear plant operator have an on-site emergency response plan approved by the NRC and an off-site emergency response plan approved by the Federal Emergency Management Agency. An on-site plan addresses the safety of the plant workers and establishes procedures for shutting down the power plant and rendering it safe.

The NRC maintains numerous safety requirements for nuclear power plants, including:

- Fenced perimeters,
- Intrusion detection devices,
- Layers of access barriers,
- Armed and trained guard forces,
- Armored defensive positions,
- A comprehensive defense strategy, and
- Detailed personnel background checks.[2]

In addition, an off-site power plant emergency response plan addresses the safety needs of those who live near the facility and includes development of evacuation routes, communication protocols and so on[3]. State and local governments draft the off-site emergency response plans in coordination with one another and industry representatives. Particularly in the post-September 11 climate, the emergency response plans can become problematic and subject to political disagreements. As an example of one highly publicized disagreement among different levels of government as well as industry, in January 2003, the state of New York refused to certify the emergency response plan for the Indian Point nuclear power plant located 35 miles north of midtown Manhattan. The state refused to issue this certification because the four surrounding counties

had refused to issue their own certifications.[4] The power plant owners on the other hand claimed that the plant had met all its emergency planning requirements.

Non-Nuclear Power Plants

The vast majority of the nation's power plants use natural gas, coal or oil. In general, power plant owners are responsible for establishing and maintaining reasonable security measures for these power plants. The threat to these facilities is primarily an economic one, although public health and environmental consequences could still be significant. A large fire at a natural gas plant or a coal plant could harm public health and the environment. As discussed above, however, the economic threat posed by the loss of such a power plant is extremely significant.

Nuclear Fuel Storage and Transportation

Nuclear power plants produce nuclear waste, which includes 12-foot-long spent fuel rods. These rods are removed from the reactor every three to four years and stored on the plant site in water-cooled pools, generally designed to hold 100 metric tons of fuel rods. However, since the United States does not yet have a central storage and disposal location for these spent fuel rods, power plant owners have been forced to store increasing numbers of these rods on-site. The cooling pools originally designed for 100 metric tons of spent fuel rods may in some cases now hold up to 400 metric tons of such rods. As the older rods cooled over a period of years, it was expected that they would be moved to the central long-term storage location. When a central interim storage facility was not developed, several nuclear plants built on-site dry cask storage. These dry fuel casks are stored outside and are relatively visible, although they are contained within the security perimeter of the power plant.

Some observers voice concerns that the spent fuel rods in both the pools and dry cask storage could pose a security threat. One concern is that the more recently stored spent fuel rods could become overheated and ignite if the water-cooled facility were breached in some way. Another concern that has been raised is whether the dry casks containing older spent fuel could be breached, releasing radioactivity. The risks from these two elements of the system are under dispute among many

policymakers, the industry and advocates, with some observers suggesting that the risks of a security breach are small and the consequences uncertain.

Nuclear Fuel Transportation

Many state policymakers have focused on security concerns regarding transportation of high-level nuclear waste through their states and near major population centers. Both the federal government and the states have roles in ensuring spent fuel and high-level radioactive waste transportation safety and security.

- The NRC regulates the packaging, preparation and transfer of commercial nuclear material under the Atomic Energy Act of 1954, as amended (42 USC 2011 et seq.), and its implementing regulations found at 10 CFR parts 20, and 71-73.[5]

- The Department of Transportation (DOT), under the federal law entitled *Transportation of Hazardous Material* (49 USC 5101-5127), is responsible for ensuring the safety of hazardous materials transportation (of which spent fuel and all radioactive materials are a subset) through numerous requirements.

- The U.S. Department of Energy (DOE) manages spent fuel transportation operations.[6]

- States have a vital role in ensuring the safe transportation of spent nuclear fuel and other radioactive materials through their jurisdiction. The states work with local governments and federal agencies to prevent accidents and provide emergency response as needed. State programs for transporting radioactive materials include issuing safety permits for shipments; vehicle, driver and cargo inspections; notification requirements; highway routing designations; and emergency response preparedness and training.

Electrical Transmission Lines

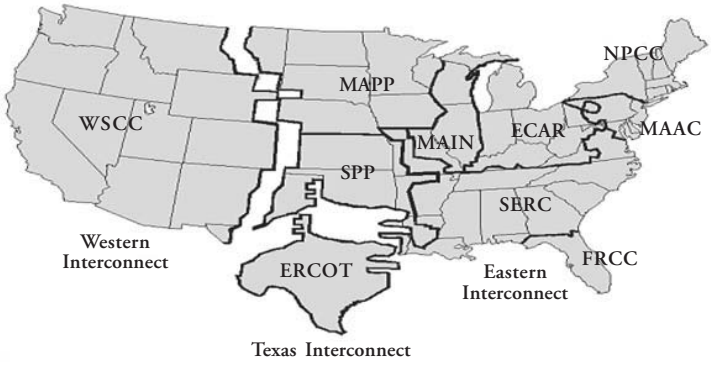
The network of electricity transmission infrastructure is an asset of the electricity system, but that network can sometimes come cascading down

(as it did in western blackouts of the mid-1990s). Power lines represent an economic threat for the most part, although the consequences of losing a major piece of the nation's transmission system also could have a major effect on public health and safety. Power lines form one interlinked network—one that is almost impossible to physically protect in the same way as one might protect a single power plant. Electricity flows over this network of power lines much like water flows through as many channels as are available to it. If one power line fails, power continues to flow through the remaining lines; however, if these become overloaded, they can overheat, sag and fail. In response, power system engineers attempt to isolate the power lines to protect the rest of the transmission system from a cascading outage. Because the electric power system is so interlinked, a failure on a single important power line can quickly cascade through the transmission system, although the potential for cascading outages depends on the configuration of individual power grids. Some observers point out that a coordinated attack at strategic points in the transmission grid could be devastating to a large portion of the transmission system.

Both government and industry have taken some steps to protect the national transmission system from a catastrophic failure. One of the most important steps that the power industry took was keep the country's electric system divided country into three large, separate power grids: the three major grids are the Western Interconnection, the Eastern Interconnection, and most of Texas, known as the Electric Reliability Council of Texas (ERCOT). Although power can flow between these interconnections to a limited degree, the three separate interconnections effectively isolate any cascading failure to one part of the country and will not affect the entire nation. The map in figure 2 illustrates the three separate electrical grids and indicates the 10 NERC (North American Electric Reliability Council) regions.

In addition, the utility industry has set up regional organizations that monitor the transmission system on a minute by minute basis, identify problems, and coordinate responses to the problems. Currently, there is uneven development of this coordinated response across the country. Thus, a continuing need exists to address not only coordination of a response but also energy system designs that make the transmission system as secure as possible through a combination of redundancy and diversity.

Figure 2. NERC (North American Electric Reliability Council) Regions



Source: Energy Information Administration, 2003.

Electrical Substations

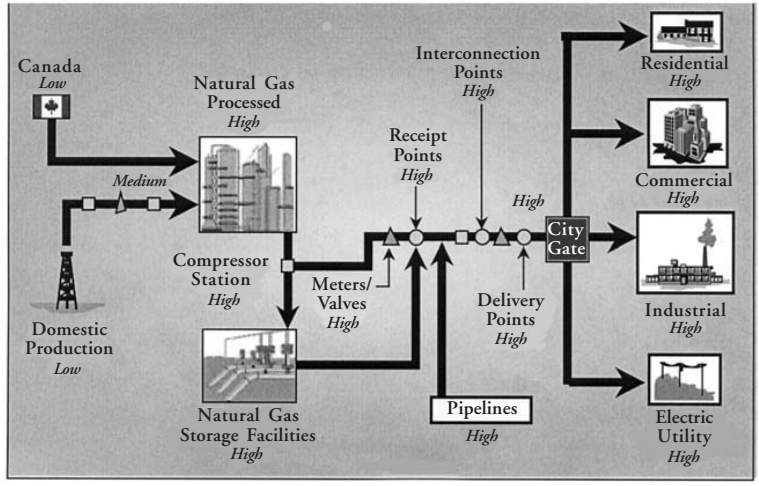
Electrical substations are a critical part of any power delivery system. The threat that results from a loss of a substation is primarily economic although, as with the transmission system significant public health impacts could also result. Substations are where transformers convert high-voltage electricity into a lower voltage that is more suitable for distribution to other portions of the grid and, ultimately, to customers. Transformers are the largest and most expensive components of a substation; each one can cost up to $2 million. It can easily take from nine months to 18 months to order and receive a new transformer. Other critical substation components such as breakers, wire and insulation devices are cheaper and more easily obtainable.

The power delivery system would be much more secure if important replacement parts such as transformers were already on hand, but the cost and uncertain need for these transformers remains a barrier to stockpiling them. Industry, with the leadership of the North American Electric Reliability Council, is now studying and attempting to develop a response to this issue.

Natural Gas System

The natural gas system is subject to numerous vulnerabilities from production to distribution, as indicated in figure 3 and subsequent sections. Figure 3 labels the vulnerability of each element of the natural gas production and delivery process as low, medium or high. This figure indicates that the natural gas system is most vulnerable after the gas is compressed into high pressure form for transportation and storage. These elements of the system represent both an economic and a public health risk.

Figure 3. Vulnerability of Natural Gas Production and Delivery Process



Source: National Petroleum Council, 2002.

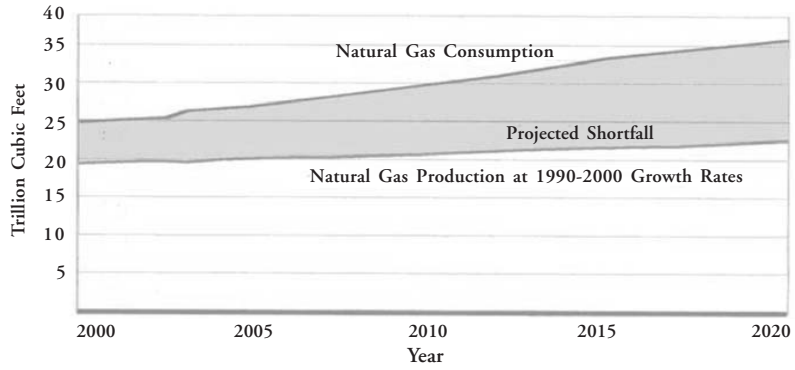
Natural Gas Storage Facilities

The natural gas network relies on pipelines, gas storage and gas imports in a super-cooled, liquid form delivered on ships. Gas companies sometimes store natural gas in this super-cooled form at minus 260 degrees Fahrenheit because 610 times more gas can be stored in this form than can be stored in its gaseous form. Gas stored or transported in this form is known as liquefied natural gas (LNG). LNG terminals and storage facilities are usually above ground and visible, which may make them

more vulnerable. LNG terminals store large amounts of fuel, representing another vulnerability within the energy system. At least 113 active LNG marine terminals or storage facilities exist in the United States as of early 2003.[7]

Because of the increasing demands on the U.S. natural gas market, the LNG marine terminals are assuming new importance. Figure 4 shows the projected trend in U.S. gas supply and demand, illustrating the growing need for gas imports of LNG.

Figure 4. Projected Trend in U.S. Gas Supply and Demand



Source: Pacific Northwest National Laboratory, 2001.

Annual LNG imports have increased by a factor of 13 from 18 billion cubic feet (Bcf) in 1995 to 240 Bcf in 2001, and now account for 6 percent of the total U.S. natural gas supply.

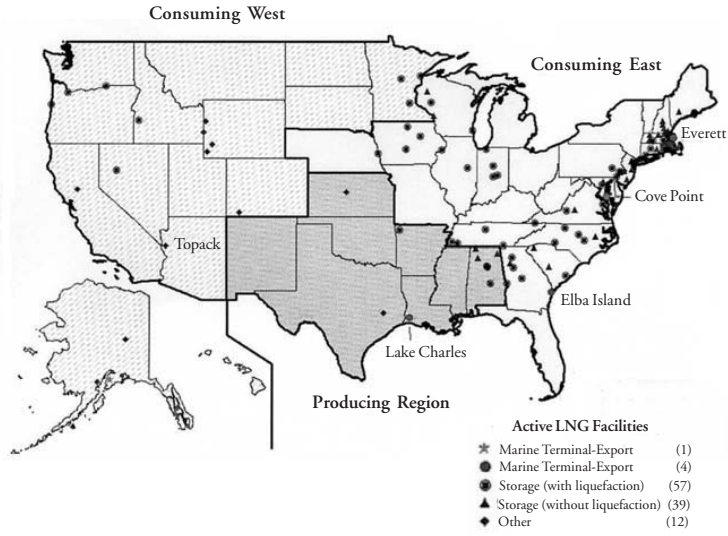
Given their typical above-ground location and important role in the energy system, LNG terminals and storage facilities represent another vulnerability within the energy system. Figure 5 shows the location of these facilities.

Natural Gas Pipelines

Natural gas pipelines serve an important role, not only for home heating and industrial uses, but to an increasing extent for electricity generation. More than 90 percent of all new power plants proposed in the United

States would use natural gas, and the dependence on natural gas is rapidly increasing.

Figure 5. LNG Terminals and Storage Facilities



Source: Pacific Northwest National Laboratory, 2001.

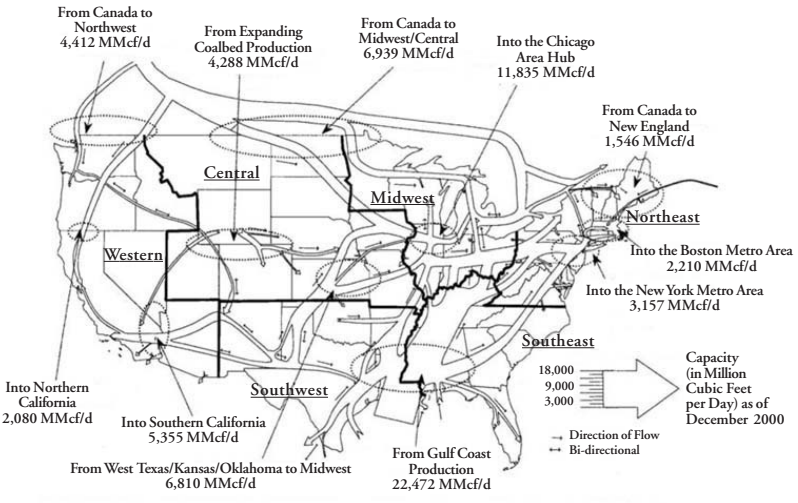
Pipelines, which typically run both above and below ground, represent a highly dispersed element of the energy system that, like transmission lines, is difficult to protect. As demonstrated in figures 6 and 7, large parts of the interstate pipeline system are located in relatively close quarters around Louisiana and Texas. Concentrated areas of the country house important parts of the pipeline network that serves much of the rest of the nation.

Petroleum

The system of drilling, transporting, storing, refining and distributing petroleum products is complex and dispersed across a wide geographic region. Different parts of the system are subject to different threats because of the concentration of products or processes in some cases, or the geographic isolation in others. The risk associated with petroleum is primarily economic, although the public health and environmental risks

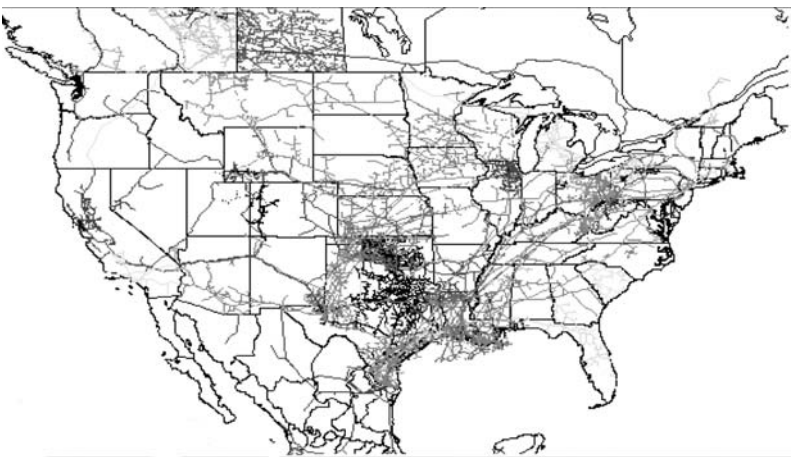
can be important in some situations as well, particularly related to transportation of liquid fuels over the nation's road system.

Figure 6. U.S. Pipeline Distribution



Source: Energy Information Administration, 2002.

Figure 7. U.S. Pipelines



Source: Energy Information Administration, 2002.

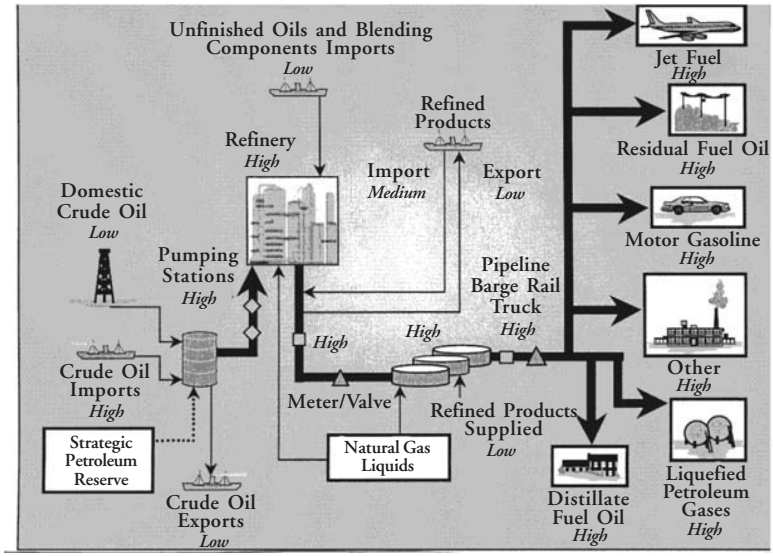
Oil Transport and Storage

Petroleum products are stored in large tank farms normally located near the population centers that serve as the market for those products. Disruptions to these tank farms pose not only an economic threat to the markets they serve but they are also a potential public safety and environmental hazard.

Oil pipelines pose an entirely different, though primarily economic, threat because of the near impossibility of securing or protecting the entire network of pipelines. The Alaskan oil pipeline is one example of a pipeline that is important to the nation's economy and its oil supply, yet is nearly impossible to defend in its entirety.

Some elements of the petroleum industry are more subject to threat than others, as shown in figure 8 and subsequent sections. In Figure 8, the vulnerability to attack of each element of the petroleum production process is labeled as low, medium or high.

Figure 8. Relative Vulnerabilities of Segments of Petroleum System and Products



Source: National Petroleum Council, 2002.

Fuel Oil

Some electric utilities use petroleum-based fuel oil to power their generating plants, but the main use for fuel oil currently is for home heating. Home heating oil is produced at refineries or is imported. Fuel oil is important throughout the United States, but the New England home heating market is particularly dependent on it for home heating. In fact, 63 percent of New England homes use fuel oil for heating, as compared to only 16 percent for the nation as a whole. 55 percent of New Englanders also use fuel oil for water heating compared to 8 percent of all households in the rest of the nation[8].

On July 10, 2000, President Clinton directed the Department of Energy to establish the Northeast Heating Oil Reserve. The reserve is intended to reduce the risks that home heating oil shortages present, such as the ones experienced in December 1996 and January-February 2000. The maximum inventory of heating oil in the reserve is 2 million barrels. The Department of Energy believes that a 2 million barrel reserve would provide relief from weather-related shortages for approximately 10 days; the amount of time it takes ships to bring heating oil from the Gulf of Mexico to New York Harbor. This reserve inventory was acquired by exchanging crude oil from the Strategic Petroleum Reserve for heating oil[9]. Figure 9 shows the storage capacity and locations of the Strategic Reserve.

Figure 9. Storage Capacity and Locations of Strategic Reserve (in thousands of barrels)

Terminal Operator	Location	Week Ending Jan. 3, 2003
First Reserve Terminal (Hess)	Woodbridge, N.J.	1,000
Williams Energy Services (formerly Wyatt Morgan Stanley)	New Haven, Conn.	500
Motiva Enterprises LLC (Equiva)	New Haven, Conn.	350
Motiva Enterprises LLC (Equiva)	Providence, R.I.	150
		Total 2,000

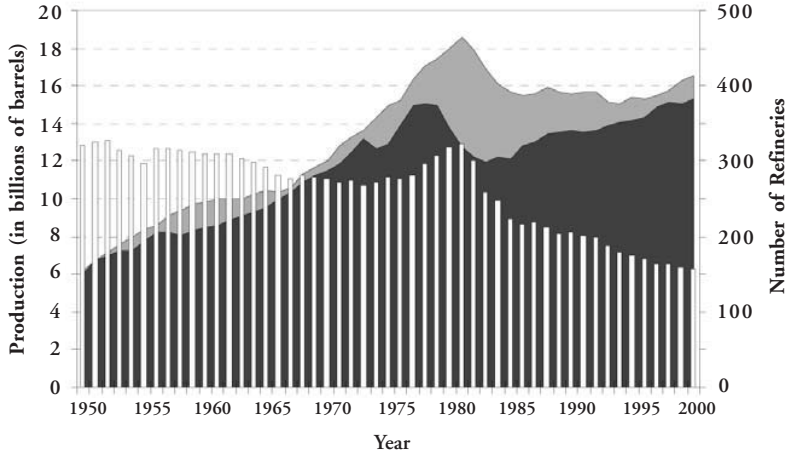
Source: Energy Information Administration, 2002.

Refineries

Oil refineries are another critical part of the nation's energy infrastructure. Refineries transform crude oil into many different products. A barrel of crude oil can be converted into propane, various grades of gasoline, naphtha, diesel fuel, jet fuel, fuel oil and asphalt. Thus, disruption in refinery production affects not only the gasoline supply and price, but also the production of other products from home heating fuel to electricity production. Security improvements at refineries are rather expensive. The CEO of Conoco Phillips reported in a March 2003 speech that security upgrades at a single refinery had cost approximately five million dollars.[10]

The oil refining business has undergone a far-reaching transformation during the past 50 years. Since 1980, the total number of refineries in the country has declined from more than 300 to about 150, while the total producing capacity of the refineries has remained steady. As shown in figure 10, the net effect has been a consolidation in the industry and fewer, larger refineries. The bars represent the declining number of refineries; the shaded area charts the refinery production capacity.

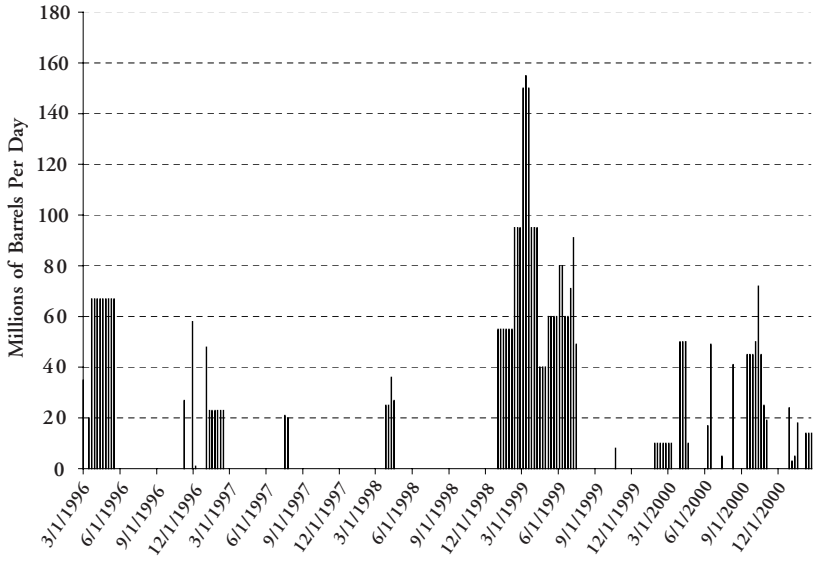
Figure 10. Capacity and Number of U.S. Refineries



Source: Stillwater Associates, 2002.

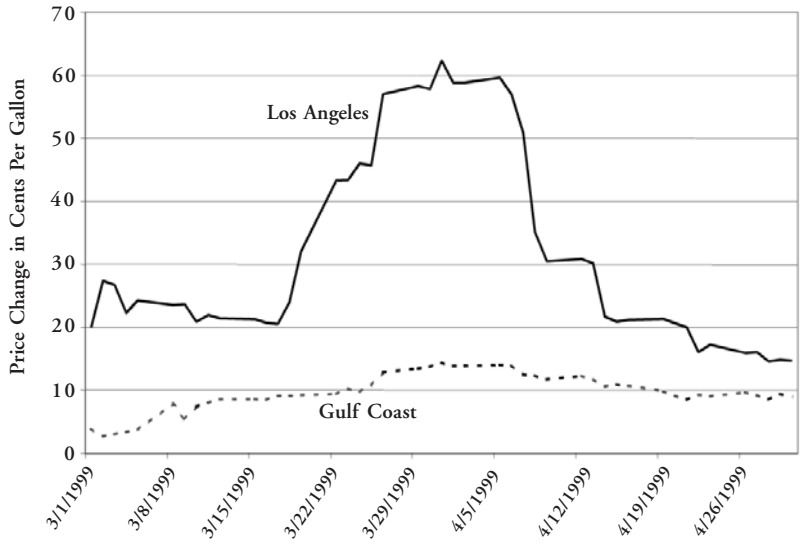
From a security perspective, the larger, more concentrated refineries may pose increased risks since an outage at one large refinery will have a more significant effect on the oil market than would an outage at a smaller refinery (figure 11). Figure 12 shows the effects on gasoline prices (only one of the products that refineries produce) that refinery outages in California had in March and April of 1999. In addition to these examples of refinery outages, other regions are also susceptible. For example, during 2001, three instances of refinery fires and outages in Illinois caused price spikes in the Midwest.

Figure 11. Refinery Outages



Source: Stillwater Associates, 2002.

Figure 12. Fuel Prices, March 1, 1999, to May 2, 1999



Source: Stillwater Associates, 2002.

Environmental Standards, Refining and Energy Security

Refineries are also subject to a number of environmental regulations. Many states now require particular fuel mixtures-often referred to as boutique fuels-in order to meet air quality standards. As a result, not every refinery can supply gasoline to every state. California, for instance, requires a high-quality fuel to meet its air quality standards. Only certain companies and refineries have made the investments necessary to supply the California market. As a result, two things have occurred: 1) only a certain, restricted number of refineries within the United States can serve the California market, and 2) California is now served increasingly by tankers carrying fuel from foreign sources that can produce fuel to meet its specifications. Numerous other states also have put fuel quality requirements in place, although California's standards are the most stringent. Figure 13 shows the various fuel requirements across the nation. While some states have established these fuel requirements for important air quality reasons, it is important to be aware of the potential energy security implications of relying on a small number of refineries.

Figure 13. Special Fuel Requirement

20 Different Fuel Formulations are Required in the Shaded Areas of this Map

Source: Exxon/Mobil, 2002.

Cyber Security and Telecommunications Systems

Cyber security refers to the security of the computer systems that operate power transmission lines and networks, gas pipelines, or the controls in other energy systems like refineries. According to a June 2001 report from the National Petroleum Council, the FBI reports that cyber criminals have penetrated, to some degree, almost all of the Fortune 500 corporations, costing the American economy approximately $10 billion per year[11]

According to the same report, a " … failure in the telecommunications infrastructure will create significant impacts to the oil and natural gas industries because of local and wide-area networks interconnecting new economy systems."[12] Cyber security is particularly important for network industries such as pipelines or electric transmission systems. Cyber attacks are dangerous mostly for economic reasons; any attack that causes an energy system to fail could cost businesses a great deal of money. A cyber attack is even more dangerous and disruptive in combination with a physical attack on the energy system.

All of the nation's critical infrastructures have a common dependency on information technologies and telecommunications systems. The introduction of, and dependency on, cyber technologies and telecommunications systems introduce new risks to the nation's energy system, even as they vastly increase the business efficiency of those systems. This increasing reliance on electronic technologies results in new threats and vulnerabilities because the development and adoption of processes to ensure security have not kept pace with the adoption of the new technologies. In this new business paradigm, individuals and groups can simultaneously attack multiple sites.[13]

The risks that cyber attacks pose are partly technical, caused by poorly designed encryption and access technology. Just as important however, is the human dimension of cyber security; people who should not have access to an energy system sometimes acquire such access. Internal policies that govern system access for terminated employees, for instance, become very important.

Cyber security becomes even more difficult in the newer, more open energy business environment. As the Federal Energy Regulatory Commission, industry and states all begin adopting measures to make the energy business more competitive, government and industry will adopt new cyber security measures. Electric utilities that own transmission systems are now required to allow other companies access to those lines and, in some cases, have turned over the management of those lines to independent entities. Open access to pipelines and power lines has become a central element of both state and federal governments' policy of introducing competition into the energy business. This competition and open access now mean that more people have access to the system. Broader access will bring with it new security and business challenges. As many utilities change their business policies to allow greater reliance on outside vendors, they also may invite new people and organizations into their previously private sphere of information. The trend toward a more open company architecture and culture offers both business advantages and poses new security risks.

4. Priority Setting, Planning and Threats

At first observation, the U.S. energy system is widely dispersed, highly interconnected and, therefore, vulnerable to a planned attack or natural disaster. It is an overwhelming and nearly impossible proposition to consider defending the nation's entire energy system with guards or surveillance. Instead, energy security implies a process that relies on two principles: priority-setting and a combination of diversity and redundancy.

Priority-Setting

Some facilities that are critical to the entire system are highly vulnerable. Certain natural gas pipelines, transmission lines, LNG facilities and power plants are critical to the function of the energy network. Other facilities may be important because of their potential threat to public health in the case of a disaster. A well-developed energy security system will use a process of priority-setting to identify the most critical infrastructure. For instance, the energy system may be able to withstand mild disruptions to some of its transmission lines, power plants, pipelines or fuel processing facilities, but may be less prepared to withstand disruptions to other more critical facilities. Further, industry may be able to rebuild and recover from some disruptions more easily than from others. Policymakers should consider focusing security efforts on the most vital elements of the energy system.

Diversity and Redundancy

An energy system that relies on a single fuel, a single transmission line or even a single computer or telecommunication system is inherently more

vulnerable than one that relies on a diversity of, and redundancy among, some resources. This implies that there is value in planning an energy system that achieves resiliency through diversity and redundancy. This concept is explored in greater detail later in the document.

The Threats

Threats to the energy system encompass much more than terrorism; although terrorism adds an entirely new set of risks to energy policy. Many of the elements of a terrorism response plan apply equally to recovery from natural disasters or from human-caused accidents. The results and devastation can be similar no matter the cause of the event.

Disaster recovery plans that states, industry and the federal government develop to address natural disasters often can work effectively in the event of terrorism; however, these plans often need to be updated. The threat of terrorism also adds new urgency and a new element to the planning process that already has been developed for natural disasters or human-caused accidents.

Part II

State Issues and Policy Options to Address Energy Security

The state role in energy security is fourfold.

- Lead where necessary and coordinate with other levels of government and the private sector.

- Beware of vulnerabilities and develop policies appropriate to reducing those vulnerabilities.

- Develop well-coordinated emergency response plans to recover from disasters as quickly as possible.

- Support coordination of industry and government efforts. States will not wish to develop new rules and regulations that have the unintended effect of actually hindering private or other sectors' energy security efforts.

States have many options at their disposal to address energy security, and these fall into two broad categories:

1. Prevention and planning, and
2. Emergency response.

Energy security policy touches upon many existing energy-related policies to some degree. In general, state policymakers will want to focus on the following policy areas.

- Jurisdiction of federal, state and local governments;
- Freedom of information issues;
- Paying for energy security;
- Emergency management and response;
- Regional energy policies;
- Cyber-security issues in energy;
- Energy system diversity and redundancy;
- Distributed energy;
- Energy efficiency and responsive demand for electricity;
- Energy facility siting;
- Energy/environmental policies; and
- Energy/transportation policies.

The remainder of this section includes an in-depth discussion of each of these issues and offers examples and models of what a state can do.

5. Jurisdiction of Federal, State and Local Governments

Jurisdictional issues define who does what in a time of emergency and who is responsible for ongoing security, planning, regulation and oversight. This section defines very briefly many of the roles that federal, state and local governments perform. In some cases, the roles overlap; in others, clear jurisdictional authority exists. In still other areas, jurisdiction may not be so clear and the roles and responsibilities of local, state and federal governments often conflict or overlap. For example, when a natural gas pipeline exploded in August 2000 near Carlsbad, N.M., the initial response was from local, state and company officials. Shortly afterward, the Office of Pipeline Safety, the National Transportation Safety Board and the Environmental Protection Agency responded. At one point, more than six different agencies were at the site. Although it is not necessarily a problem for several different agencies to respond to an incident, the New Mexico explosion shows the need for those different agencies to communicate with one another.

Table 1 is intended to show the major roles and responsibilities of various agencies, not to define every role in energy security.

Table 1. Jurisdiction Over Energy Security

Function	Local	State	Federal
Nuclear Power Plant Oversight	X, for emergency response	X, for emergency response	X
Ongoing Guarding of Energy Facilities	X	X, if National Guard	X, in rare circumstances
Freedom of Information Requests	X	X	X
Awareness of Energy System Vulnerabilities	X	X	X
Pipeline Safety			X (Federal DOT)
Retail Electricity Products and Fuel Diversity	X (for municipally owned utilities; for local government purchases)	X (through utility commissions, portfolio standards, incentives, funding and state purchase.	X (through tax incentives, federal government purchases)
Energy System Planning	X (limited role)	X	X
Siting Certification	X (in home rule states)	X	X (for interstate pipelines only)
Emergency Management and Response	X	X	X
First Response to Emergency	X		
Oversight of Energy Security Costs	X (for municipal utilities)	X (through utility commissions under statutory authority)	X (for FERC-jurisdictional costs)

Source: NCSL, 2003.

This table suggests two major conclusions:

- Local, state and federal governments share responsibility for most elements of energy security. Local government sometimes serves only as first responder, but sometimes is also the utility as well, as is the case with municipally owned utilities.

- To maximize efficiency, local, state and federal governments need to collaborate, share information, and develop coordinated plans and responses.

Table 1 does not indicate the industry's role in energy security, which permeates every level of the discussion. It also does not deal with the need for regional collaboration among states in such issues as energy emergency preparedness and response or energy system planning. Ultimately, the differing jurisdictional authorities will need to be resolved through communication and planning—most likely through an emer-

gency response planning activity that involves local, state and federal officials. Ultimately, each level of government plays an important role in response, planning, detection and recovery. Local governments are first responders and assist in recovery. State governments play roles in planning, safety, environmental and emergency preparedness, freedom of information and decisions about who pays for security. The relationships among the different levels of government must be clearly defined.

Federal Role

The Department of Homeland Security: The Homeland Security Act of 2002 (PL 107-296)

Established by the Homeland Security Act, the new Department of Homeland Security (DHS) will play a critical role in energy security. The mission of DHS is to prevent terrorist attacks within the United States, reduce the nation's vulnerability to terrorism, minimize damage and assist in the recovery from terrorist attacks, perform emergency planning for natural and manmade crises, ensure that homeland security efforts do not diminish overall economic security, and pursue terrorism linked to the drug trade.

The act does not give DHS primary responsibility for investigating and prosecuting acts of terrorism. This activity generally remains within the jurisdiction of federal, state and local law enforcement agencies (Appendix A contains selected text of The Homeland Security Act).

DHS Structure

DHS has an organizational structure with five major directorates:

- Border and Transportation Security;
- Management;
- Emergency Preparedness and Response;
- Chemical, Biological, Radiological and Nuclear Countermeasures; and
- Information Analysis and Infrastructure Protection.

The Information Analysis and Infrastructure Protection division will use modeling and simulation technology to analyze infrastructure needs and set priorities for security measures. DHS will focus this work on vulner-

able targets with catastrophic potential, such as nuclear power plants, chemical facilities, pipelines and ports. The agency will then establish policy for standardized, tiered protective measures that address the perceived threats.

DHS will attempt to streamline and coordinate homeland security efforts between the federal, state and local governments. Aside from the five main directorates, the department will contain an intergovernmental affairs office—the Office for State and Local Coordination—to manage DHS activities that relate to state and local officials, agencies, the private sector and other entities.

This office will provide state and local officials one primary contact for matters related to training, equipment, planning and other critical needs such as emergency response. The office will coordinate communication systems that the federal government uses to communicate with state and local authorities. States will be able to provide recommendations for improving homeland security strategy. State interests will find an advocate in the Office for State and Local Coordination for federal funding of their activities. This office also will distribute research, technical support, warnings, and other information to state governments.[1]

Other Federal Roles in Energy Security

- Since 1954, the federal government has regulated nuclear facilities. The Energy Reorganization Act of 1974 transferred regulation of nuclear power plants from the Atomic Energy Commission to the Nuclear Regulatory Commission. In some cases, by signing formal agreements with the NRC, states can assume regulatory responsibility over certain small quantities of nuclear material and byproducts. Thus far, 32 states have undertaken this responsibility. These arrangements are closely monitored and assisted by the NRC.

- The Federal Energy Regulatory Commission is responsible for approving rates for security-related measures at power plants or in power lines, especially for merchant power plants. FERC also issues siting certificates for natural gas pipelines and regulates hydro dam safety.

- The federal government plays an important role in funding and performing research and development for new energy security technologies.

Several federal agencies share responsibility for energy security, and since the creation of the new Department of Homeland Security, the roles of the federal agencies have shifted even more. Many agencies play some role in energy security; however, the three described below are particularly important.

The *Department of Homeland Security* will serve as the agency most directly concerned with direct threats to the nation's energy infrastructure, vulnerability assessments and responding to those threats.

The *Department of Energy* works to address strategic energy security issues through its efforts on electricity transmission, fuel diversity, energy supplies, research and development and other similar issues.

The *Federal Energy Regulatory Commission* examines the economic issues affecting security costs for utilities under its jurisdiction, focusing on approval of security related costs in rates and hydro dam safety.

The *Department of Commerce Office of Pipeline Safety* regulates safety-related issues in pipelines. *The Transportation Security Administration with the Department of Homeland Security* is taking on new roles in pipeline safety that are yet to be defined.

6. Freedom of Information Issues

State policymakers are surprised to discover that one of the most important state policy issues related to energy security-and, indeed, related to security of almost all infrastructure-is who shares what information with whom, and under what circumstances. These policies are usually governed by state and federal statutes and are known collectively as freedom of information act (FOIA) policies.

Why Are Freedom of Information Act Policies Important?

FOIA policies are important to energy security and the security of other critical infrastructure for several reasons, among which are vulnerability information, ratemaking, and the public's right to know about threat and vulnerabilities.

Vulnerability Information

One of the most important elements of preparing for the possibility of an attack on infrastructure is to understand that infrastructure's vulnerabilities. Yet, because a detailed understanding of the vulnerabilities in an energy system would be useful to someone plotting to disrupt the energy system, it is important to control that information carefully. This issue is relevant at the moment in several contexts.

- The U.S. Department of Energy has performed numerous vulnerability studies of the energy system in many states around the country. Yet the Department of Energy must be careful about how and

with whom it shares this information. Its caution in sharing this information with state or local governments stems from the department's concern that sharing this information would subject it to state freedom of information procedures, thereby making it accessible to the public.

Similarly, many utilities also are reluctant to share data with any level of government because they also are concerned that it could be available to enemies/attackers as a result of disclosures required under FOIA. A 2002 survey of public utility commissions, conducted by the National Regulatory Research Institute (NRRI), concluded that many utilities were highly reluctant to share their security data, plans or vulnerability assessments with their own state commissions.[1] Some municipally owned utilities, which are both operating utilities and units of government, may have special issues as they attempt to protect sensitive information while complying with FOIA laws. Water utilities have also performed their own vulnerability studies, and many share information with the U.S. Environmental Protection Agency. Like the U.S. DOE, EPA must be careful about sharing its information about the vulnerability of water systems with state governments for fear of it falling into the wrong hands.

- Some observers suggest many government or industry Web sites that contain critical information about the nation's energy infrastructure could be used to plan an attack. On the other hand, government entities need to share this information with each other. To handle an emergency, it is often critically important that state and local officials have information from other government entities. The National Strategy for Homeland Security recommends that state and local governments establish a secure Intranet to communicate classified federal information to state and local entities.[2]

Ratemaking

State public utility commissions typically approve rates for utilities under their jurisdiction after a lengthy review of the components of the utilities' costs. This involves an occasionally lengthy administrative hearing process. This process is legislatively mandated, usually required under administrative code. Other intervenors in utility rate cases also typically have access to large quantities of information about utility expenditures. This infor-

mation helps both the commissions and the utilities to determine what should or should not be included in the utility's rate base.

One concern about utility investments that are classified as "security-related" is that the overly broad FOIA exemptions might not allow information about security investments to be available to the commission. This lack of information makes the regulator's job of approving cost recovery for prudent investments more difficult.

The Public "Right" to Know vs. the "Need" to Know About Threats and Vulnerabilities

Many advocates of a liberal policy toward freedom of information suggest that it is important for the public to have access to information about the threats that confront the nation. One column suggests that, " ... in the United States, and elsewhere in the world, the public has a right to know information that may directly affect their lives ... If a safety report says that it's too easy for someone to break into a chemical plant and cause an accident, the local residents should know about it ... "[3]

At heart, the question facing policymakers is one of balance. What process can state policymakers use to balance the public's right to know about the threats and about the costs involved in meeting those threats with the possibility that the information itself will increase the threat and perhaps expose the country to greater risks?

How Have States Addressed FOIA?

Since September 2001, states have begun to look carefully at their freedom of information act policies. Many have attempted to balance the public's right to know with concerns about security.

Numerous states have exempted energy security-related information from state FOIA requirements, have exempted it under certain circumstances, or have given state agencies the authority to exempt themselves from FOIA requirements. Although some states may choose to further clarify their exemptions for disclosing energy security information, it appears that many states now have exemptions in place to address some of the utility and federal concerns about information disclosure.

- After the September 11 terrorist attacks and as of mid-2003, 15 states—Alaska, Arkansas, Colorado, Connecticut, Delaware, Idaho, Kansas, Louisiana, Maine, Maryland, Massachusetts, Missouri, Rhode Island, Ohio and Wyoming—altered their FOIA laws to exempt security-related information.

- Eleven other states—Florida, Michigan, Nebraska, Nevada, New Hampshire, New Jersey, North Carolina, Oregon, Utah, Virginia and Washington—already had comprehensive information disclosure statutes in place that addressed terrorism concerns.

- Some states—including California, Georgia, Hawaii, Illinois, Indiana, Kentucky, Mississippi, Oklahoma, South Carolina, Tennessee, Texas, Vermont, West Virginia and Wisconsin—and the District of Columbia—designate information as confidential if other statutes (including federal statutes) or regulations do so. New York has numerous general exemptions in its statutory language. These include exemptions for disclosures that would endanger the life and safety of any person, or any information that would jeopardize an agency's capacity to guarantee the security of its information technology assets, including infrastructure.

- Six other states—Alabama, Arizona, Iowa, New Mexico, North Dakota and South Dakota—require specific exemptions to prevent disclosure of sensitive security-related information but do not do so for information related to energy security.

In the NRRI utility commission survey, most respondents indicated that they offer FOIA protection for sensitive utility security information, although 22 percent did not. In addition, most respondents said their commission had experienced no change in security authority after September 11, 2001.

The test of these state laws may come from the courts and from attempts to designate with specificity what information fits into the categories defined in the laws. In general, the courts tend to give deference to security concerns in such situations.

Kansas

Kansas has taken steps to remove sensitive energy-related information from the public record. Many states have "open record" or "freedom of information" laws that require certain data to be available to the public. Sensitive information regarding power plants and transmission lines is subject to these laws in many states. One problem with this policy is that states and the federal government may be discouraged from coordinating and sharing vital information with one another if they know the public will have access to it. Kansas protects this sensitive information by exempting it from the public record. Kansas lawmakers believe that doing so can facilitate coordination between different levels of government and help protect the power system from likely attack. Legislation enacted during the 2002 session amends the Kansas Open Records Act to exempt from the public record all records that pose a likelihood of revealing security measures taken to protect the energy generation, transmission and distribution system, water and wastewater systems, and communications infrastructure.

Michigan and Wisconsin have taken or are considering similar action. The text of their FOIA statutes or bills is included here.

Michigan

On March 29, 2002, the governor approved Act No. 130 of Public Acts of 2002, effective May 1, 2002. This act amended the Michigan Freedom of Information Act (FOIA) Act 442 of 1976 (15.2 MCL) by providing protection from disclosure information relating to critical infrastructure protection. The new exemption, Section 13(1)(y), states:

"Records or information of measures designed to protect the security or safety of persons or property, whether public or private, including, but not limited to, building, public works, and public water supply designs to the extent that those designs relate to the ongoing security measures of a public body, capabilities and plans for responding to a violation of the Michigan anti-terrorism act, chapter LXXXIII-A of the Michigan penal code, 1931 PA 328, MCL 750.543 to 750.543z, emergency response plans, risk planning documents, threat assessments, and domestic preparedness strategies, unless disclosure would not impair a public

body's ability to protect the security or safety of persons or property or unless the public interest in disclosure outweighs the public interest in nondisclosure in the particular instance."

Wisconsin

A bill introduced in the 2003 session of the Wisconsin Legislature would amend statute Section 1. 19.36 (10) to give an agency authority to exempt certain information from FOIA requirements. The bill reads as follows:

"**Security information.** An authority may withhold access to any record or portion of a record containing information regarding security measures to protect the safety of the plant, equipment, employees, or customers of a person that generates, transmits, or distributes electricity, transports or distributes natural gas, operates a public water system, or provides telecommunications or sewer service."

Federal FOIA and Interaction with State FOIA Laws

According to the Homeland Security Act, critical infrastructure information that customarily is not in the public domain will be exempted from federal FOIA laws in certain cases. When a utility or other entity voluntarily submits information to the Department of Homeland Security, and the information is accompanied by a request that it be protected according to the act, the information will be exempt. Once exempted, the information cannot be used " ... directly by such agency, any other federal, state or local authority, or any third party, in any civil action"[4] if the information was submitted in good faith. However, the act does not amend the Freedom of Information Act, and does not affect use in criminal cases.

Section 214 (a) (1) (E) of the Homeland Security Act sets the same requirements for information that DHS subsequently gives to a state or local government or agency. If information meeting the requirements is transmitted to state or local government, it will be exempt from disclosure at the state level unless the person or entity that submitted the information approves disclosure. Finally, this section specifies that the information cannot " ... be used other than for the purpose of protecting

critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act."[5]

According to the Homeland Security Act, information about homeland security must be shared between federal agencies and the appropriate state and local personnel via systems that are accessible only to this personnel and that can transmit classified as well as unclassified information.

7. Paying for Energy Security

Energy security may be costly and will require energy companies to make new investments in energy facilities that they had not previously expected. Some of these investments may be for new equipment and others may be for additional employees and security personnel. Some companies -such as oil companies-that operate in competitive markets and are not price-regulated, will make the investments as they see fit and will seek to lower costs and increase efficiency elsewhere in their business or perhaps raise prices to the extent the market allows. Companies that operate in regulated, monopoly markets -including gas, telecommunications, electric and some water companies- operate in a more public environment where state or federal officials oversee the rates they can charge. The questions that surround how the states should allow utilities to recover their security-related costs dominate the debate about paying for energy security. Three major questions are important:

- What categories of costs should utilities be allowed to recover?
- What mechanism should be used to allow utilities to recover their security-related costs, and how quickly should they be able recover those costs?
- How much detailed oversight and approval should utility commissions have over cost recovery?

What Categories of Costs Should Utilities Be Allowed to Recover?

Most of the costs associated with energy security fall into one or more of the following categories:

- Vulnerability assessments,
- Information management and intelligence,
- Threat detection,
- Physical security,
- Cyber security,
- Consequence management, and
- Event mitigation.[1]

Utilities face potentially enormous financial outlays for energy security. In general, state policymakers can expect that utilities will undertake some action that falls into one or all of the above categories. The Edison Electric Institute estimates that total costs could exceed several billion dollars for a variety of security-related investments. The array of security related investments is wide, and includes investments in overstocking replacement parts for electrical substations and new guards and surveillance measures. Having spare equipment on hand is one way to mitigate damage that outages may cause and create redundancy within the power system. Stockpiling certain vital equipment is expensive (e.g., transformers can cost up to $2 million each), and power providers are hesitant to purchase additional parts because they are uncertain when, if ever, they will need the equipment, and how they will recover these costs. It can also take a long time to deliver vital replacement parts. Utilities must make the case that their expenditure is both related to security and prudently incurred before the utility commission allows the expenditure into the utility's rate base.

State utility commissions examine security-related costs, as they do all costs, with an eye to determining if they are prudent investments. The definition of prudency is extensive, but basically it involves determining that the investment was reasonable under the circumstances that the utility could know, or that were knowable at the time the utility made the investment.

Finally, utility commissions generally approve costs that state or federal agencies mandate. However, utilities incur some security costs voluntarily. These costs now constitute the majority of security-related costs and their recovery is subject to greater question. A large majority of respondents to the NRRI utility commission survey reported having no guidelines for determining the prudence of security investments. Nine per-

cent of respondents presently are developing guidelines. NRRI suggests that utilities and utility commissions undertake a collaborative dialogue about the range of approaches available to provide and strengthen security. This dialogue could result in agreements about what the utility can do to improve security, and about what costs the commission is likely to approve. The certainty that such a collaborative dialogue could produce may also speed the process of making the electricity network more secure. In general, the regulators' role is to review utility decisions, but not to substitute the commission's judgement for the more detailed knowledge held within the utility itself.[2]

The question that state policymakers must ask is which of those costs are part of a new set of investments necessary for energy security, and which investments would have been made anyway, as part of the normal course of upgrading and maintaining equipment. Most respondents to the commission survey indicated that utilities had undertaken security-related investments on their own accord, not in response to state or federal mandates. Most respondents reported that utilities in their states had not filed for security-related cost recovery. Of all the commissions, 33 percent noted that "a few" utilities had come forward with filings for cost recovery. States and utilities must agree upon which equipment or other investments qualify for treatment as a prudent investment in security.

What Mechanism Should Be Used to Allow Utilities to Recover Their Security-Related Costs, and How Quickly Should They Be Allowed to Recover Those Costs?

Utilities earn money by making investments that regulators approve, and then by including those investments in a set of costs known as their rate-base. Regulators allow utilities to recover the costs in the rate base over some period of years plus a reasonable return on their investment, usually in the range of 12 percent per year. Utilities occasionally must undergo a lengthy process known as a rate case before they can include many of their investments in the rate base. One way for utilities to recover their investments in security is for them to wait for the next rate case, in the meantime expecting that they will keep their system secure as part of their duty to reliably deliver power.

Rate cases have been rare during the past decade, and it is now common to find utilities that have not gone through a rate case for five years or more.[3] This means that there can be a lag during which utilities make investments that are not included in their rates until the next rate case. For major investments such as those proposed for energy security, this regulatory lag can be problematic. The rate case structure leaves utilities in the difficult position of considering investments without knowing if regulators will later allow them to recover those investments at all. This uncertainty may actually discourage them from spending money on security.

Another approach is quicker and also can be accomplished under the traditional regulatory process with little or no legislative intervention. This process is based on the theory allowing utilities to recover Construction Work in Progress (CWIP), or certain costs that they incur in building a power plant, but prior to the plant entering service. The CWIP mechanism allows utilities to recover certain costs upon demonstrating that they have, indeed, made the investment and that it fits into the proper category. Through this mechanism, regulators might set out a category of costs that would qualify for this CWIP-like process, and utilities then could make such investments with the knowledge that they could later recover the costs.

Some utilities operate under a rate cap or rate freeze—a mechanism under which the utility has agreed not to increase its rates. Sometimes this rate cap is a hard cap that allows for no surcharges or pass-throughs of expenditures. In other cases, it is a soft cap that allows the utility to charge for some extraordinary items.

In either case, states have options. In the case of a soft cap, utilities can be allowed to pass their security-related costs to their customers in a special surcharge (similar to a fuel adjustment charge). In the case of a hard cap that does not allow for additional pass-throughs, the commission might allow the utility to keep track of its expenses through what is known as a deferred charge, and pass them through at some later date.

How Much Detailed Oversight and Approval Should Utility Commissions Have Over Cost Recovery?

State policymakers, primarily through their utility commissions, must balance the need to oversee the utilities they regulate with the desire to allow them to manage the details of their security measures. Utilities do this with some assurance that the regulatory commissions will approve their prudently incurred costs. Each state will need to develop its own approach to how it allows utilities to recover their security-related costs.

Condition	Solution Menu
Regulated utilities, no rate cap or freeze	1. Address security costs in next rate case. 2. Allow commission to allow quick pass-through of security costs through normal regulatory process. 3. Enact legislation to ensure recovery of security-related costs, with specified commission oversight.
Regulated utilities with soft rate cap	1. Address security costs in next rate case. 2. Allow commission to allow quick pass-through of security costs through a special surcharge. 3. Enact legislation to ensure recovery of security-related costs, with specified commission oversight.
Regulated utilities with hard cap	1. Enact legislation to ensure recovery of security-related costs, with specified commission oversight. 2. Allow commission, through regulatory process, to set up a "deferral" account for utility to recover prudent costs at a later time.

In every situation, it may be prudent for the state and the regulated utilities to collaborate and to determine a common strategy for addressing security issues. This common strategy could make utilities more certain that they, would later be able to recover their costs.

Other Considerations In Paying for Energy Security

Municipal, county and state-owned utility systems, as well as customer owned systems, must also pay for security investments. Many of these entities own large power plants and operate sizeable portions of the nation's transmission grid. In general, the rates that these non-profit entities charge are not subject to a public utility commission's scrutiny, therefore many of the approval issues described above do not apply to them. State policymakers should be aware, however, that the security investments that the public power entities must make will be comparable to those that investor owned utilities must make. These investments will have an effect on the rates that these utilities charge their customers.

Kansas Enacted Legislation that Addresses Cost Recovery for Energy Security

In 2002, Kansas enacted legislation (HB 2374, KSA 66-1233) to address the way in which utilities recover their security investments. The Kansas Energy Security Act encourages power providers to purchase extra equipment by allowing them to recover "reasonable" costs associated with enhancing security measures. Once the Kansas Corporation Commission (KCC) approves the costs, companies can pass them on to customers through the billing process. As a further security measure, the charges must be rolled into the rate and may not appear as a line item on the bills. Kansas lawmakers believe it is important to keep information regarding the amount and method of cost recovery confidential so that no one can determine exactly where and how much money is being spent to bolster security.

Some oppose this method, asserting that the extra security measures should be visible on electric bills because customers have the right to know what they are paying for. The sponsor of the legislation argues that costs related to security enhancement should remain secret and be rolled into the rates just as is already done with many taxes and other charges.

8. Emergency Management and Response

Guidelines for States

States have learned some valuable lessons about planning for energy-related emergencies. The following is a set of guiding principles for successful planning in this area.

1. Keep plans as flexible as possible. Each energy emergency is unique and different measures will be required in every case.

2. With adequate oversight, allow decisions to be made at the lowest possible level of government. Many decisions can be handled entirely at the local level or by coordination between local authorities, and state and federal agency personnel. It is probably not appropriate or feasible for the governor's office to make every important decision in an emergency.

3. Before an emergency occurs, it is imperative to have a written plan and for key players to know each other. Staff turnover means that newly hired people might be faced with handling an emergency and an established plan will provide them the guidance they will need. Key decisionmakers should meet on a regular basis so that they can identify one another in an emergency. They should also conduct joint emergency management exercises. They should not meet each other for the first time during an emergency situation.

4. In developing a plan, government must work with industry experts. The expertise of those working in the oil, electricity, natural gas,

propane and other critical infrastructure industries is crucial to developing comprehensive plans.

5. Energy flows through an interconnected network (see figure 1, page 9), so coordination with other states and the federal government is necessary. Very few energy emergencies affect only one state and they are likely to ripple across borders. State governments may need financial and administrative assistance from the federal government should a major emergency occur.

6. Dialogue with the public is crucial. Modern communication technologies enable information to travel rapidly and as a result, needless panic can spread easily. Emergency coordinators should have a public presence to calm fears that arise from misinformation. If unchecked, this kind of panic can lead to real crises such as the lines for gasoline that formed shortly after September 11, 2001.

Source: Greg Guess and John Davies, Kentucky Division of Energy, January 2003 interview with author.

Long before September 2001, federal law encouraged states to design plans for preventing and addressing energy emergencies. The Department of Energy made receipt of its State Energy Program (SEP) funds contingent on the preparation of these plans. (DOE currently awards SEP funds that support a wide variety of energy-related programs to every state.) In some states, emergency plans may require updating to reflect a rapidly changing industry and concerns about national security.

Hawaii

The state of Hawaii's Energy Council provides a model of a successful emergency preparedness and management structure. The Council was established in 1992 in the wake of Hurricane Iniki, which devastated the Island of Kauai. This model was then adopted at the state level and has demonstrated flexibility and effectiveness in its ability to adapt and evolve according to emergency planning and security needs- most recently by coordinating critical infrastructure protection against acts of terrorism.[1]

Michigan

As ordered by the governor, Michigan currently is evaluating the security of critical energy infrastructure and updating its emergency response plan to ensure that the plan is current and comprehensive.

The Michigan Public Service Commission (PSC) has primary responsibility for state energy-emergency planning and response. The PSC continuously monitors the state's energy supply and infrastructure, noting circumstances that could lead to energy emergencies. The PSC coordinates communication among the three levels of government—federal, state, and local—and with the various segments of the energy sector. In the case of a shortage or other emergency, the PSC develops and administers contingency plans.

Michigan Energy Emergency Act

Public Act 191, enacted in 1982, is the Energy Emergency Act. This act established the Energy Advisory Committee, which is responsible for notifying the governor of an impending energy emergency. The Energy Advisory Committee includes the directors of the departments of commerce, public health, transportation, agriculture, state police and the chair of the Michigan Public Service Commission, who serves as chairperson for the advisory committee. The committee's recommendations are based on information from the Michigan Public Service Commission, other state agencies, federal agencies, and other sources. Either based on the committee's notification or the governor's initiative, the governor may declare a state of energy emergency. This allows the governor to order mandatory state actions such as ordering restrictions on the use and sale of energy resources and restricting indoor temperatures, lighting levels and hours of operation for public, industrial, school and commercial buildings. Restrictions can also include limits on driving and on speed limits. The governor can also issue executive orders to implement this act, and can suspend certain statutes or state agency rules.

After the governor declares an energy emergency, the official state of emergency continues for 90 days or until the governor declares that the emergency has ended. If the Legislature finds that the state of emergency should be extended beyond 90 days, it can approve an extension by a concurrent resolution.

Emergency Management Act

If an emergency becomes more serious than what can be handled by executive orders and proclamations, the governor may declare a state of disaster. At this point, the state's Emergency Management Act takes effect. Disaster-related activities then fall under the jurisdiction of the Emergency Management Division, a main division of the Department of State Police.

According to the Emergency Management Act, Public Act 390, the director of the Department of State Police is responsible for:

- Making recommendations to the governor and implementing the orders and directives of the governor in the event of a disaster.
- Coordinating all federal, state, county and municipal operations within the state.
- Administering state and federal disaster relief funds.
- Assigning general missions to the National Guard or state defense force to assist disaster relief operations.
- Maintaining a division within the department to coordinate the predisaster emergency service activities of federal, state, county and municipal governments.

Source: Michigan Emergency Management Act 390, 1976.

Natural gas and electricity companies in Michigan have also developed plans for dealing with disruptions. The Public Service Commission approves these plans and oversees them as the utilities implement them. The emergency electricity procedures define how utilities should handle long- and short-term shortages or outages. The Commission penalizes utilities if they do not deliver gas to customers during times of emergency.

In January 2002, Michigan's governor issued an executive directive establishing the Michigan Homeland Security Task Force. Its purpose is to bolster that state's security by coordinating all the activities of federal, state, local and private organizations. One of the four main committees

of the task force is the Critical Infrastructure Protection Committee, which includes PSC staff.

The Energy Subcommittee of the Critical Infrastructure Protection Committee, is currently surveying security measures and exploring ways to improve the security of all systems that produce or distribute energy, including petroleum products, natural gas and electricity. This includes coal shipments, generation plants, transmission systems, natural gas compressor stations, natural gas and petroleum pipelines, petroleum refineries and barge shipments, propane storage, and a variety of distribution and control systems. Once complete, the Energy Subcommittee will submit the review to the Critical Infrastructure Protection Committee then to the state's Homeland Security Advisory Council.

Regional Cooperation-Interstate Compact
Michigan entered into the Emergency Management Assistance Compact (EMAC) on Jan. 9, 2001, (see pages 63-65).

Kentucky

Kentucky's energy emergency plan follows a less rigid set of protocols than Michigan's and offers a range of options for dealing with individual incidents.

The Division of Energy (the state's energy office) is located within the Department of Natural Resources. Revised Statute 224.10-100, subsections 28 and 29, require the Kentucky Division of Energy (KDOE) to develop and implement programs for the development, conservation and utilization of energy in order to meet human needs and support the state's economy. KDOE is required to maintain information on energy supply, demand and conservation. The statute also requires KDOE to formulate a contingency plan for coping with energy shortages.

KDOE has worked with other local, state and federal agencies and with private industry to fulfill this mandate. The main energy emergency plan, an appendix to the state's general Emergency Operations Plan, is used in severe and/or long-term energy emergencies. The plan, which was updated in 2001, is known as Annex P.

Annex P

Annex P provides a framework for coordinating and organizing the state's energy resources during an emergency. It assigns responsibility to government entities and provides a set of optional measures for emergency management. Options, which focus on managing limited supplies and reducing demand, are laid out for outages or shortages of electric power, natural gas, propane and liquid fuels. Because each energy crisis is unique, Kentucky has laid out a non-prescriptive plan that allows options to be tailored to each emergency. During a declared emergency, the governor would choose from among the various options.

Kentucky's plan states that energy emergency management should be based on the following:

a. The top priority should be to meet the needs of activities that are essential to the health and safety of the citizens of Kentucky.
b. Emergency responses should rely on the market to the greatest degree possible to meet demands.
c. The responses should rely on voluntary actions to the greatest degree possible, but certain conditions will inevitably call for mandatory requirements.
d. Responses should stress voluntary cooperation with energy suppliers.
e. State personnel and resources should be used to the highest degree possible.
f. Coordinate information and press releases to ensure that state agencies speak with a common voice.
g. Keep citizens informed of the situation and most recent developments to minimize panic buying and reactive behavior.

The director of the Kentucky Division of Emergency Management is the governor's representative for coordinating all emergency responses and, as such, works directly with local governments. Annex P states that, during an energy emergency, this director will receive guidance and recommendations from the Kentucky Energy Resources Management Board (ERMB).

Energy Resources Management Board

When an energy emergency is declared, the Energy Resources Management Board meets to assess the situation and advise the governor. Officials in the affected localities also coordinate directly with the board, which is chaired by the secretary of the Kentucky Natural Resources and Environmental Protection Cabinet. Permanent members include the Public Service Commission, the Kentucky Division of Energy, the Department of Mines and Minerals, the Department for Surface Mining Reclamation and Enforcement, and the attorney general. The board's chair has coordinates its activities with the Division of Emergency Management and the governor. If warranted by a severe energy emergency, other agencies may join the board.

The board works with various advisory committees that have expertise on energy issues to develop policies to respond to emergencies. Advisory committees include the Gas and Electrical Services Committee, the Oil and Gas Production Committee; the Coal Production Committee; the Petroleum Products Committee and the Consumer Affairs Committee. The committees, which consist largely of industry representatives, meet at least once per year or during emergencies that affect their particular industry sector.

Kentucky's planning process emphasizes the importance of decisions made at the lowest level of government. The advisory committees and member agencies of the ERMB, aided by the Division of Emergency Management, often can handle emergencies with local governments. In appropriate cases, ERMB officials believe this practice works more effectively than involving the governor and formally activating the board.

Energy Emergency Standard Operating Procedures

The Kentucky Division of Energy maintains a guidebook of standard operating procedures that contains contact information for each government entity that would assist in an energy emergency.

Regional Cooperation-Interstate Compact

Kentucky is a member of the Emergency Management Assistance Compact, which is described later in this report (see pages 63-65).

Emerging Issues: Transportation of Fuels

In early 2003, the ERMB began work with the state Department of Transportation to ensure that, during an emergency, drivers of fuel trucks—especially propane—can legally work extra hours. In some cases, when emergency fuel supplies are needed, trucking companies find their drivers bound by restrictions on operating hours that make it difficult to deliver all the necessary supplies. This issue affects numerous other critical infrastructure providers across the country, especially utilities.

9. Regional Energy Policies

All states are dependent on others for their energy supply. The infrastructure of shipping, pipelines, power plants and transmission lines is vital to every state, but each can exercise control over only a small portion of this system. Long-term planning of the energy system, as well as resiliency during emergencies, will likely require a greater level of interstate coordination.

Long-Term Planning

Although each state has policymaking autonomy, it is important to understand the regional nature of the energy system. For example, fuel oil is extremely important for home heating in the Northeast. In recognition of the region's unique dependency on this fuel, the federal government established emergency fuel oil reserves for the region. In another example of multi-state needs, a transmission system that delivers power from supplier to customer will almost certainly cross state boundaries. This issue is particularly important for states such as North Dakota, which has a declining population and wants to export power to markets in non-neighboring states.

State governments can initiate multi-state cooperation, but federal action is sometimes required. To help with regional planning of the transmission system, the Federal Energy Regulatory Commission has proposed regional transmission organizations (RTOs). FERC Order 2000 asked all transmission-owning utilities, including non-public utilities, to place their transmission facilities under the control of an appropriate RTO. The proposed structure is intended to make the transmission system more organized and efficient-especially in congested areas such as the Northeast-while simultaneously improving power markets and competition.

Resiliency During Emergencies

Interstate cooperation on energy emergency management is important for two reasons:

1. Major energy shortages or disasters will likely affect more than one state.

2. Few individual states are likely to have all the required resources and trained personnel on hand to deal with a major crisis. Federal aid may be slow to arrive or may not be awarded at all.[1]

The energy network is a complex web of exports, imports and shared dependency on infrastructure. An energy-system emergency in one state will almost certainly affect others. A natural gas pipeline rupture in Texas could cause shortages in Oklahoma, and the loss of a transmission line in Washington could cause blackouts throughout the western grid. An oil spill off the coast of South Carolina might not be large enough to warrant federal help, but perhaps be large enough to overtax South Carolina's resources. North Carolina and Florida could assist by providing cleanup crews and supplies. Such cooperative efforts could, in fact, prevent the disaster from affecting more than one state.[2]

To enable states to communicate during emergencies, the National Association of State Energy Officials assembled a list of energy emergency information coordinators for every state and territory. Coordinators may contact each other using an e-mail listserve. In case of an energy emergency, coordinators are expected to submit a written report to the Department of Energy and to neighboring states.[3]

The Emergency Management Assistance Compact is a tool for regional cooperation in the aftermath of almost any kind of disaster. Although states have not yet used the compact, it is a helpful tool they can turn to in the future.

The Emergency Management Assistance Compact

The Southern Governors' Association developed the Emergency Management Assistance Compact (EMAC) in 1992 in the wake of Hurricane

Andrew. EMAC includes legal mechanisms for reimbursement and for tort liability issues. The compact also outlines the types of assistance and equipment that can be shared. It establishes an implementation plan under which member states agree to standard operating procedures for requesting and providing assistance. It provides uniform procedures for many aspects of emergency management, including evacuations and interstate recognition of professional licenses. However, the compact does not mandate any state to provide assistance-this remains optional. Perhaps the most important result of the compact is that member states know the expectations and responsibilities involved in helping one another. This assistance can be vital if federal aid is delayed or unavailable.

The National Emergency Management Association, the professional association of state emergency managers, administers EMAC. A $1,000 optional annual membership fee is requested. For a state to join, the state legislature must ratify the compact by passing the compact's language into state statute. The compact has been endorsed by the following bodies: the Southern Governors' Association, the Midwestern Governors' Conference, the Western Governors' Association, the Adjutants General Association of the U.S., the Midwestern Legislative Conference, the National Governors' Association, the New England Governors' Conference, the National Guard Bureau, and the Federal Emergency Management Agency.

Recently, states have used the compact to help each other after the September 11 and Columbia space shuttle disasters. Since Congress approved it in 1996, 47 states, the U.S. Virgin Islands, Puerto Rico and the District of Columbia have ratified EMAC. As of Feb. 18, 2003, Wyoming's bill had passed the Legislature and was awaiting the governor's signature. Wyoming would become the 48th state to join. The only two states who have not joined the compact are California and Hawaii.

Virginia, Maryland and the District of Columbia developed their own shared emergency response strategy after the evacuation gridlock of September 11. The Regional Emergency Coordination Plan allows the three to share resources and communications. It is designed to work in coordination with plans such as EMAC.

In 1998, the Conference of New England Governors and Eastern Canadian Premiers established the International Emergency Management Assistance Compact (IEMAC), which is a mutual aid compact very similar to EMAC. However, IEMAC formalizes the process for New England states to aid or receive aid from the eastern Canadian provinces. IEMAC recognizes that, in many emergencies, New England states have more connection with eastern Canada than with many U.S. states.

10. Cyber-Security Issues in Energy

State utility commissions have some oversight over cyber-security preparedness, largely focused on ensuring that the utilities under their jurisdictions have taken appropriate precautions for cyber security. In general, the commissions can work with industry to set requirements to guide security procedures through standards. State commissions may, for instance, establish a requirement that utilities submit a set of policies to the commission for approval. Commissions may ensure that utilities not only develop plans that the commission reviews for adequacy, but also that the utilities are diligent in following, implementing, reviewing and updating those plans.

State policymakers also may address liability for outages and, in particular, for cyber breaches related to outages. Before writing a policy for cyber insurance, the insurance company will audit the utility's operations and perform a subsequent audit at various points. One policy option is to either require or encourage utilities to carry such insurance.

The North American Electric Reliability Council

The North American Electric Reliability Council (NERC) has operated since 1968 as a voluntary organization to promote electric system reliability and security—one dependent on reciprocity, peer pressure, and the mutual self-interest of all those involved.

In promoting electric system reliability and security, NERC:

- Sets standards for the reliable operation and planning of bulk electric systems.
- Monitors, assesses, and enforces compliance with standards for bulk electric system reliability.
- Assesses, analyzes, and reports on bulk electric system adequacy and performance.
- Coordinates reliability standards and reliability matters with regional reliability councils and other organizations.
- Coordinates critical infrastructure protection of bulk electric systems.
- Enables the reliable operation of interconnected bulk electric systems by facilitating information exchange and coordination among reliability service organizations.

The growth of competition and the structural changes taking place in the electric industry have significantly altered the incentives and responsibilities of market participants to the point that a system of voluntary compliance is no longer adequate. In response to these changes, NERC is transforming itself into an industry-led, self-regulatory electric reliability organization that will develop reliability standards for the North American bulk electric system.

NERC has taken responsibility for coordinating a great deal of the electrical infrastructure security and is now developing new policies that focus particularly on cyber-security issues, as well as some other related security issues. NERC set up a task force to address all security issues known as the Critical Infrastructure Protection Advisory Group—CIPAG. The new policies and standards that NERC is developing are meant to ensure that companies have a basic security program in place, and that that program protects the electric grid and the electricity market from events that could have a wide-ranging, harmful effect on grid operations. NERC is, as of early 2003, considering a set of cyber-security standards to which power companies would need to adhere. These standards would require companies to create a cyber-security program, to identify vulnerable cyber assets, to perform proper personnel training and develop procedures for access to information and to facilities, as well as a number of other areas such as periodic testing, incident response and recovery plans.

The Federal Energy Regulatory Commission regulates the wholesale electric power market and also addresses some security issues. One recent proposed rulemaking (Docket No. RM01-12-000) refers to the NERC standards process described above, and would require utilities to have a tariff on file with the FERC certifying that the companies comply with the NERC standard.

States' efforts on cyber security must be made in the larger context of the NERC requirements, perhaps filling in gaps where national standards may be insufficient for local circumstances.

11. Energy System Diversity and Redundancy

The U.S. energy infrastructure relies heavily on a few fuels to power its transportation sector, to heat its homes and businesses, to fuel its industrial energy needs and to generate electricity. Within each of these sectors and within certain geographic regions, the energy infrastructure is still dependent on individual energy sources. For example:

- The U.S. transportation sector is more than 95 percent dependent on petroleum.

- More than 95 percent of all new electricity generating plants will use natural gas.

The energy market tends to encourage an energy system that is least expensive in the short term, which is why relatively inexpensive natural gas power plants now are predominant among the new power plants. Yet, for price and security reasons there may be value to the overall energy system in increasing the diversity of fuel supplies. Diversity among methods of delivering energy can also increase competition.

- Texas regulates natural gas pipeline prices because there is no realistic alternative means to deliver natural gas. Texas does not regulate oil pipeline prices in some part because it is possible to transport oil using trucks instead of pipelines.

- In some instances, land-line phones and wireless phones have begun to compete. This not only gives giving customers additional choices, but also increases the security of the system through diversity.

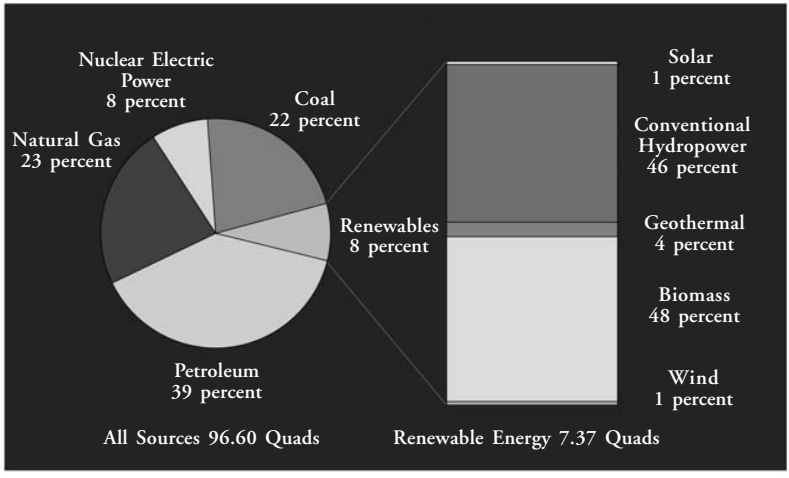
- In certain constrained situations, tap water, trucked water and bottled water are alternative means to serve similar markets.

- Energy systems that rely on a combination of fuels, resources and delivery methods may be inherently more secure than energy systems that rely on single fuels and single, concentrated delivery methods.

The goal of fuel diversity requires a mix of long-term strategies and a careful balance between government intervention in energy markets and policies that allow those markets to operate independent of significant government influences.

State policies can encourage diversity in energy supplies. They have tended to do so by encouraging renewable energy, which currently represents a relatively small proportion of the nation's total energy use. States also can encourage new investments in coal, nuclear or other technologies if they so desire. Figure 13 illustrates the sources of fuel for all energy consumed in the United States.

Figure 13. Sources of Fuel for U.S. Energy

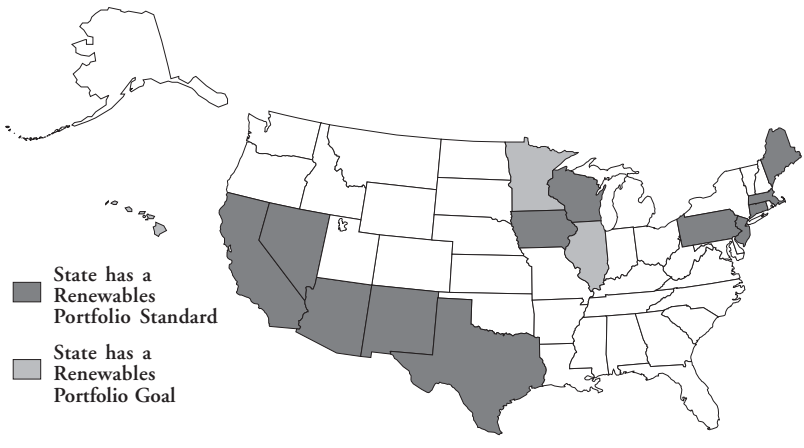


Source: Energy Information Administration, 2000.

Typical policies that states use to encourage fuel diversity are the renewable energy portfolio standard and the public benefit fund. Both are discussed below.

The renewable energy portfolio standard requires energy retailers to provide a specific percentage of their total power from renewable resources. Figure 14 illustrates the 12 states that, as of early 2003, had a renewable energy portfolio standard in place.

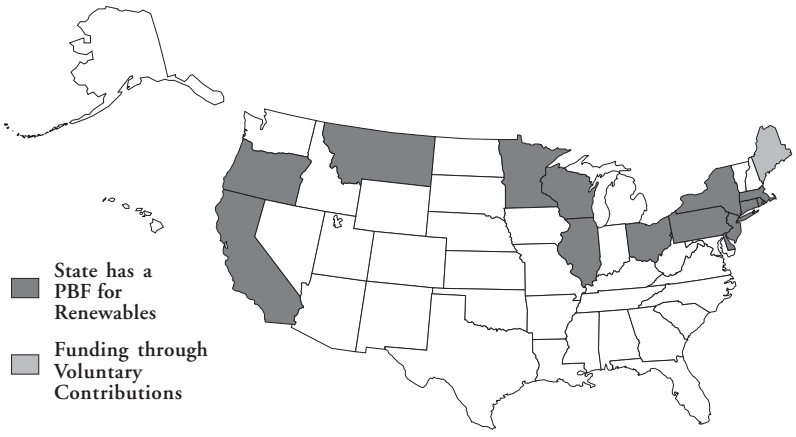
Figure 14. States with Renewable Energy Portfolio Standards



Source: NCSL, 2003.

The public benefit fund is another mechanism to support fuel diversity. A public benefit fund—also known as a system benefit fund—is a small charge (usually less than one-tenth of 1 cent per kilowatt hour) that is added to every customer's electricity bill. The funds accumulate in an account that either the state, the state's utilities or a nongovernmental entity manages. That entity uses the funds in the way that it sees most useful to promote a number of energy functions, including renewable energy, energy efficiency, and research and development. These funds typically, but not always, support renewable energy. Illinois, for instance, maintains a fund that supports both Illinois coal development and renewable energy. Figure 15 shows which states have public benefits funds for renewable energy.

Figure 15. States with Public Benefits Funds (PBF) for Renewable Energy



Source: NCSL, 2003.

12. Distributed Energy

Distributed energy refers to small-scale energy systems that are located close to where customers use the electricity. Distributed energy is small, usually less than 10 megawatts (although definitions vary), and stands in contrast to central station power generation techniques. Central station generation refers to large power plants that generate power in one location and then send it over wires to customers on the other end.

Distributed generation refers to many different energy technologies—including diesel engines and gas engines—that have been operating for decades. It also refers to a number of new technologies such as gas microturbines (essentially smaller, scaled-down versions of new gas combustion turbines that generate electricity), fuel cells (that generate power through an electrochemical process), and small-scale wind generation or solar electric panels.

The benefit of these smaller, distributed resources is that they offer an alternative to the power grid. If the electricity transmission grid goes down, customers do not lose power if they have an on-site generator. Distributed resources provide diversity and decentralization to the electricity delivery system. They benefit the customers who have installed them but do not replace the bulk power system.

However, the electric system was not built to accommodate large numbers of these small generators. As a result, utilities face some technical hurdles before their systems can accommodate many of these independent systems. One challenge that utilities face is if large quantities of small generators start their systems and begin delivering power into the grid from numerous distributed points.

These technical issues are being addressed through a set of technical standards set up by the Institute of Electrical and Electronics Engineers (IEEE). This technical research organization of the electric utilities' is also addressing technical issues such as how to create and manage small micro-grids of distributed generation resources.

Another issue surrounding small-scale generators is air emissions, which vary tremendously among the distributed generation technologies. In general, the oldest, most common and best established distributed energy technologies emit more pollutants than do the most advanced, but less common, technologies. State policymakers seeking to promote energy diversity through new distributed generation technologies also will need to consider the related policy issues involving air quality.

13. Energy Efficiency and Responsive Demand for Electricity

Many states encourage energy customers to use less energy through a combination of technology measures such as new, efficient light bulbs, appliances, and motors and through behavioral measures like turning off lights in unoccupied rooms. Some states and power companies also promote demand response. Demand response programs compensate customers who reduce their demand at particular times, either in response to an increase in price or at the request of the power system operator. Demand response is especially valuable at the peak times of a day or year when the electric system is making use of all, or nearly all, of its available capacity and thus when the cost of producing electricity is relatively high. In general, these efficiency, conservation, and demand response programs exist for a combination of economic and environmental reasons.

Such programs can also contribute to energy security and energy emergency response in a number of ways.

- Energy efficiency reduces demand on power plants and power transmission lines. To the extent that power lines are not already running at or near the upper limits of their capacity, and under normal operating conditions, power system engineers have more flexibility to reroute power flows over a variety of lines or to increase the output of underutilized power plants. If lines and power plants are already running at or near their capacity limits due to high electric demand, power system engineers do not have this flexibility. Flexibility to

rely on a variety of energy sources and power delivery routes becomes critical in an emergency that takes certain power lines or plants out of commission.

- Demand response programs can contribute to emergency response. When California and some other parts of the western United States faced a crisis in the power system's ability to deliver power at reasonable prices in 2000-2001, demand response became very important. Many large customers agreed to reduce their total demand for power in exchange for a pre-arranged payment from the utility. It was cheaper for the utility to purchase demand reductions from customers (thus freeing up energy for more valuable uses) than it was for the utility to acquire new supply. In the West, these demand reductions remained in effect for extended periods of time, many months in fact, until the crisis was resolved (that is, until the water resources in the north and gas supplies in the southwest returned to normal). In the Northeast, demand response programs are also in effect, and they enable the system operator to shift customers' demand for power from peak to off-peak hours (times when the power system typically runs at far lower than its total capacity). While power was cut off in some communities at some hours, this disruption would have been more frequent, and possibly uncontrolled, without demand response.

These demand response programs can be an important part of an emergency response plan, and can provide one way to continue to deliver power even when the power fails at one generating station or along a critical transmission path.

14. Energy Facility Siting

Most states maintain an energy facility siting function with varying levels of input from local governments. Yet, these siting boards and the decisions they make can have important implications for energy security. State laws that govern siting transmission lines can have a surprising impact on energy security. State siting law rarely considers energy security. States may add security to the list of considerations for siting authorities to examine when issuing siting certificates.

Power lines represent one crucial part of the power infrastructure, and siting authority is one major area through which states exercise significant influence over the location of power lines. Local communities closest to new power lines often object to the notion of a utility building lines nearby because they do not like the way power lines look and are concerned that the lines may reduce their property value.

There are broader security related concerns to consider, as well. These fall into the general category of redundancy and diversity.

- *Redundancy*: New power lines can increase the reliability of the electric system by reducing the strain on existing lines by providing new paths over which power can flow should the primary path go down.

- *Diversity*: In some cases, the need for new power lines can be balanced against alternatives that can reduce the load on the electricity system. These alternatives, including both distributed generation and energy efficiency, may reduce or delay the need to build new transmission and, in some cases, may be inherently more secure than reliance on the grid.

Security is rarely a consideration in power plant, power line or other energy facility siting. A typical facility siting statute will require the siting authority to consider other important issues. The Connecticut siting statute, for instance, describes the authority to balance the numerous factors:

> "To provide for the balancing of the need for adequate and reliable public utility services at the lowest reasonable cost to consumers with the need to protect the environment and ecology of the state and to minimize damage to scenic, historic, and recreational values; to provide environmental quality standards and criteria for the location, design, construction and operation of facilities for the furnishing of public utility services at least as stringent as the federal environmental quality standards and criteria, and technically sufficient to assure the welfare and protection of the people of the state; to encourage research to develop new and improved methods of generating, storing and transmitting electricity and fuel ... with minimal damage to the environment and other values described above; ... to require annual forecasts of the demand for electric power, together with identification and advance planning of the facilities needed to supply that demand and to facilitate local, regional, state-wide and interstate planning to implement the foregoing purposes."[1]

Nowhere in this description of balancing state goals is energy security mentioned, nor is it generally mentioned in other state statutes. State policymakers may consider adding an energy security element to the list of considerations for siting power plants or power lines.

Finally, states may consider a related issue. Because of the difficulty in siting new power lines, pipelines and telecommunications cables, some people have proposed creating utility infrastructure corridors, or single concentrated channels through which these lines can pass. While this approach might ease the siting process, it may also make the transmission system more vulnerable by reducing the inherent advantage of geographical diversity.

15. Energy and Environmental Policies: Interactions with Energy Security

For air quality reasons, some power plants that release more pollution are permitted to run for only a certain number of hours or days per year. During an extended power shortage, however, a state air quality agency may be pressured to extend the permitted hours of operation for all available power sources. Extended hours could result in more emissions from polluting power plants. If this became necessary for a prolonged period of time due to a disruption in the energy system, the state might encounter air quality problems and could exceed pollution standards laid out in the Clean Air Act. Although it appears that no states have yet needed to extend the operating hours for large plants, at least one state has experienced the air quality effects of smaller generators in electricity crises.

Many experts predicted the California energy crisis would culminate in a long summer of blackouts in 2001. Governor Gray Davis faced pressure to allow all backup generators (many diesel-fired) to run during serious outages, but opposition from environmental groups prevented this. However, a few months earlier, a power outage on the campus of the University of California at Berkeley prompted the use of 29 diesel-fired backup generators to light hallways and perform other important functions. According to Environmental Defense, several 911 calls were made about the resulting plumes of smoke that were seen across the campus.[1]

Vital locations such as hospitals have backup generators, most of which are usually diesel-fired. The California Air Resources Board classifies die-

sel exhaust as a toxic contaminant. Studies conducted by the South Coast Air Quality Management District, the California Air Resources Board, and EPA have recently found that diesel exhaust contributes to more than 70 percent of all cancer risk from airborne toxins. Newer diesel engines are less polluting, but diesel generators are in some cases less tightly regulated than are large power plants.

As they address the issue of energy security, state policymakers may wish to consider the environmental effects of handling major power outages and shortages. State regulators issue permits that limit the number of hours that a power plant can operate during the year. Generally, regulators base the number of hours that they permit a power plant to operate on its emissions. The reliability of the power system may come into conflict with environmental regulations when certain, baseload power plants go off line. If the power plant that goes off line happens to be a new, efficient and low-emitting facility and the power plants that would replace it are older and higher emitting facilities, state environmental policymakers and regulators face a dilemma. Do they increase the number of hours that they allow the higher-emitting facility to operate in order to keep the electric system running, or do they seek some other solution?

A long-term alternative could include incentives for cleaner large-scale generation, certain types of lower-emitting distributed generation facilities; increased use of new, cleaner diesel fuels (such as low-sulfur diesel or biodiesel); and more efficient engines.

16. Energy and Transportation Policies

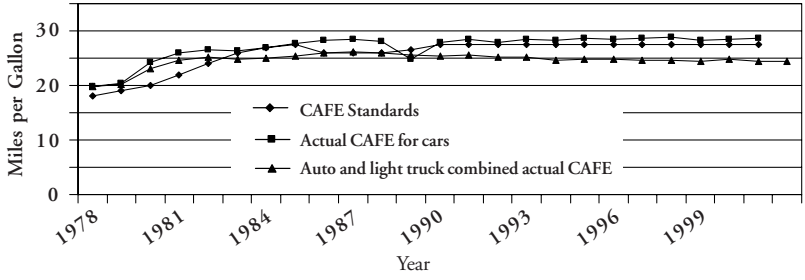
State and federal policies can foster new transportation fuel types and better vehicle efficiency. State policy may play an important role in decreasing the dependence on imported oil for transportation, but this transformation of the market will occur slowly over a number of years. Although the role of fuel efficiency is long-term and does not address the short-term catastrophic implications of a loss of energy infrastructure, these policies are worth mentioning in an energy security discussion. The federal government regulates all vehicle fuel efficiency standards leaving little direct role for the states in setting these standards.[1]

According to the American Council for an Energy-Efficiency Economy, cars and light trucks consume around 41 percent of all petroleum products in the United States and 61 percent of the total energy used in transportation. The average fuel economy in new passenger vehicles of this type declined from around 26 miles per gallon (mpg) in 1988 to 25.1 mpg in 2000. These decreases were due largely to the growing market share for light trucks and SUVs and year over year decreases in CAFE standards for some manufacturers. These changes were driven by consumer demand. During this same time, consumption of gasoline and diesel fuel increased by 19 percent due to increased vehicle use.

Increasing the fuel efficiency of passenger vehicles may be one long-term way to curb oil imports; however, low gasoline prices may be just as important a factor in gasoline use. People drive more when gasoline is cheap. Further, better fuel economy by itself has not reduced imports in the past. Even as fuel economy standards for light duty vehicles increased by 50 percent from the late 1970s through the 1980s, oil imports rose. Figures

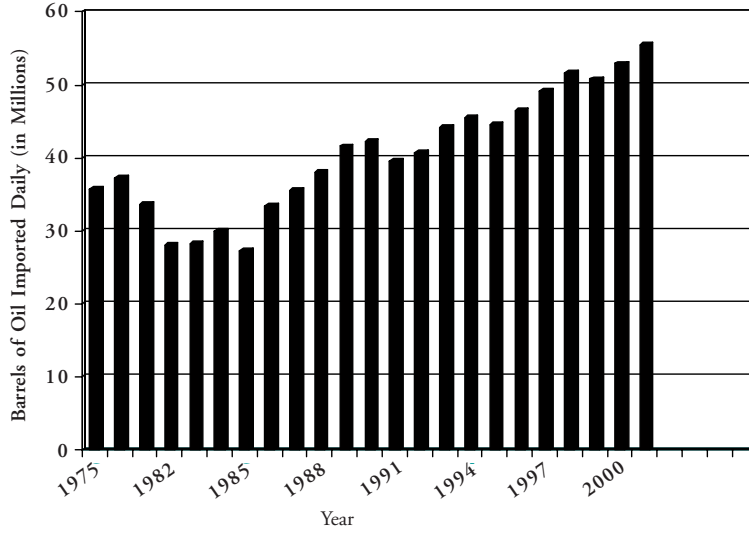
16 and 17 show this trend. Oil imports as a percentage of total oil consumption in the United States have been rising at a far greater rate than the increase in overall consumption of oil in the United States. This indicates something else is happening: oil is far less expensive to produce outside the United States than within the United States.

Figure 16. U.S. Corporate Average Fuel Economy



Source: Energy Information Administration, 2003.

Figure 17. U.S. Oil Imports



Source: Energy Information Administration, 2003.

Table 2 illustrates how certain modifications and engine technologies can greatly increase the fuel economy of passenger vehicles. Many of these technologies are featured on new vehicles.

Table 2. Technologies for Improving Passenger Vehicle Fuel Economy

Technology	Fuel Economy Improvement (Percentage)
Weight reduction	3 percent - 4 percent
Aerodynamics	0.5 percent - 2 percent
Variable valve control	0.5 percent - 2 percent
Direct injection spark ignition	5 percent - 23 percent
Other engine refinements	0.5 percent - 2 percent
Improved transmissions	0 percent - 3 percent
Hybrid powertrain—near and mid-term	7 percent - 50 percent
Hybrid powertrain—longer term	TBD

Source: NHTSA and NAS studies, 2003.

Throughout the 1990s, many states enacted policies to support alternative fuel vehicles (AFVs). These vehicles are powered by natural gas, electricity or fuels produced from crops such as soybeans, sugarcane and corn. Most state incentives have not successfully created a large market for AFVs, but more popular hybrid gasoline-electric vehicles have recently become available and these may be better equipped to increase fuel efficiency.

The AFV market has not materialized because most incentives are poorly structured and have not stimulated the private sector to build a new fueling infrastructure. The incentive programs that seem to work well are 1) focused on reducing petroleum use and emissions, 2) large and grant-based, 3) easy to administer, and 4) focus on developing infrastructure as well as vehicle acquisition.

The commitment of auto manufacturers, fleet operators, natural gas companies, electric companies and fuel suppliers is needed to support an AFV market. Although these industries have not completely abandoned AFVs, their support dwindled in the later half of the 1990s.

Hybrid vehicles, which sometimes qualify as AFVs, offer the range and flexibility that some consumers demand from traditional vehicles while

simultaneously increase fuel economy. Hybrid engines switch seamlessly between gasoline and electricity for power; and derive their electric power from the vehicle engine instead of a plug in the wall. The Honda Civic, Honda Insight and Toyota Prius are three popular versions of hybrids. Last year approximately 27,000 HEVs were sold, less than 0.1 percent of total sales. Ford and Toyota also are currently developing the first hybrid SUVs.

17. Conclusions and Action Items for Legislatures

State policymakers have an indispensable role in energy security. They oversee much of the structure that governs the preparation for, the avoidance of and the recovery from a major disruption to the energy system. Ill-conceived state policies can hinder preparedness and recovery while well-crafted policies can smooth the process. It may not be possible for state officials to prevent an attack or a disruption to an energy system, but they can certainly help in prevention and, without question, work to make response and recovery as seamless as possible. The following state action items offer guidance for state policymakers to consider. They are designed to identify where in state law and statute policymakers might look to identify energy security-related activities.

Action Items

State policymakers are seeking ways to improve energy security, but often have little knowledge of what state policies they can best focus on to do so. This section defines areas of law where state legislators can focus attention.

Seek Information and Education

Even without legislative authority, state legislators can take the initiative to visit important energy facilities throughout their state. Kansas Representative Carl Holmes, for example, has visited almost every major electric generating station in the state since September 2001. He has found this effort to be important to his policymaking role as chair of the House Energy Committee. Visits such as these facilitate information sharing

and establishing contacts and help state policymakers understand how to best assist industry in its efforts to make facilities more secure.

Review Utility Commission Enabling Statutes

State commissions are already familiar with utility contingency plans for potential disasters. As a result, commissions have the expertise to provide technical support for homeland security and law enforcement efforts. Commissions can also supply necessary information about protecting utility infrastructure, and can relay threat and warning information to smaller and rural utilities as appropriate.[1]

Integrating state commissions and state energy offices into emergency planning and response efforts is essential. A 2002 exercise discovered shortcomings in cooperation, coordination, communications, resources, command and control, and public information dissemination between the sectors participating in the exercise, including energy, telecommunications, water supply, and transportation—sectors generally within the jurisdiction of state commissions.[2] In particular, legislatures may want to determine the following:

- If the state utility commission has sufficient authority in existing law to collect information on security from regulated entities and to oversee and approve utility security plans where deemed necessary.

- The sufficiency of Freedom of Information exemptions for information submitted to the utility commission related to critical infrastructure security.

- If the utility commission has sufficient guidance, authority and oversight related to pass-throughs of security-related costs. Determine if the commission has sufficient guidance related to disclosure of such costs on customers' bills.

Identify Opportunities for Energy Efficiency and Encourage Demand Response Programs

Energy efficiency and demand response programs make electricity systems flexible and better able to respond in times of emergency.

Examine Security Implications of State Siting Law

- Determine if the state siting authority allows consideration of security issues in decisions about siting certificates.

Analyze Statutes Governing Energy Office and Duties

- Determine if the state energy office has sufficient authority and budget to:
  - Provide technical assistance to policymakers on energy technologies and practices that increase energy security;
  - Manage state and federal grants, along with other financial assistance, to encourage the use of energy technologies and practices that increase energy security;
  - If required, oversee energy emergency management function;
  - If required, oversee an energy analysis and planning function;
  - In some cases, oversee state research and development activity;
  - In some cases, perform analysis of various energy technologies such as distributed generation; and
  - Determine integration of state homeland security office with these functions.

Study Statutes Influencing Energy System Diversity and Redundancy

Determine what policies the state may wish to pursue to encourage diversity of fuels used for power generation. Such policies may include incentives for renewable energy or, in some situations, coal-based generation. Such policies also may include mandates for certain generation technologies.

Determine what policies the state may wish to pursue to encourage diversity in the delivery of energy. Such policies may include those that encourage small-scale distributed energy systems or energy efficiency measures.

Determine what policies—such as siting law or regulatory policies—may encourage redundancy in the energy infrastructure. Redundant tech-

nologies ensure minimal losses if one segment of the system is temporarily or permanently lost.

Review Statutes Governing Freedom of Information Laws (FOIA)

Determine if state FOIA laws and related regulations provide exemptions for energy security-related information. Balance such exemptions between the need for security and the public's right to know about security-related issues.

Reassess Laws and Procedures Governing Open Meetings

Legislatures must find a balance between the need for open meetings and government's own need to know about security threats. The United States Congress has processes that allow for executive sessions on certain sensitive subjects, but in many cases state government is prohibited by state constitutions from doing this. The balance between this need to know sensitive information in order to make appropriate policies, and the longstanding openness of communication between government, industry and the general public is important to maintain, but now faces new challenges and questions.

Evaluate State Liability Statutes

Examine liability on the part of utilities for harm done in the course of responding to a direct attack on an energy facility. In some cases, utilities may be reluctant to make certain security-related policies unless liability issues are addressed.

Ensure that Industry and/or State Agencies Have Conducted Appropriate Vulnerability Studies

To protect critical infrastructure, some states have conducted in-depth studies to determine security needs. After September 11, the Texas attorney general established the state's Infrastructure Protection Advisory Committee. The committee reviewed the state's infrastructure and made recommendations to help protect infrastructure from terrorism-related threats. Missouri has a similar committee. New York's Public Utilities

Commission directed utilities to do vulnerability assessments. The commission hired an independent consultant to verify the utilities' assessments and report to commissioners. New Jersey took similar action. With a comprehensive assessment of vulnerable infrastructure in hand, policymakers may find it easier to develop a plan for increasing infrastructure security.

Update Statutes Governing Emergency Response

Determine if statutes governing emergency response provide for:

- Coordination among local, state and federal levels of government;
- Coordination among different state governments;
- Coordination and information-sharing among agencies with the state and with local governments as first responders;
- Coordination between industry and state government;
- Defined duties and responsibilities for government and industry;
- Sufficient flexibility to respond to different energy emergencies; and
- Means to disseminate information to the public.

Examine Possible Unfair Pricing Legislation in Emergencies

Arkansas, California, Connecticut, Florida, Hawaii, Indiana, Louisiana and the District of Columbia prohibit companies from setting prices at unreasonable high levels during times of emergency. These pricing policies generally affect energy products—such as gasoline or diesel fuel—that are not already price regulated.

Action Items

Appendix A. Homeland Security Act of 2002, PL 107-296 (excerpts)

Excerpts from the Homeland Security Act
Section 101 of the Department of Homeland Security Act of 2002, PL 107-296:

SEC. 101. EXECUTIVE DEPARTMENT; MISSION.

(a) ESTABLISHMENT—There is established a Department of Homeland Security, as an executive department of the United States within the meaning of title 5, United States Code.

(b) MISSION—

(1) IN GENERAL—The primary mission of the Department is to—

(A) prevent terrorist attacks within the United States;

(B) reduce the vulnerability of the United States to terrorism;

(C) minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States;

(D) carry out all functions of entities transferred to the Department, including by acting as a focal point regarding natural and manmade crises and emergency planning;

(E) ensure that the functions of the agencies and subdivisions within the Department that are not related directly to securing the homeland are not diminished or neglected except by a specific explicit Act of Congress;

(F) ensure that the overall economic security of the United States is not diminished by efforts, activities, and programs aimed at securing the homeland; and

(G) monitor connections between illegal drug trafficking and terrorism, coordinate efforts to sever such connections, and otherwise contribute to efforts to interdict illegal drug trafficking.

(2) RESPONSIBILITY FOR INVESTIGATING AND PROSECUTING TERRORISM—Except as specifically provided by law with respect to entities transferred to the Department under this Act, primary responsibility for investigating and prosecuting acts of terrorism shall be vested not in the Department, but rather in Federal, State, and local law enforcement agencies with jurisdiction over the acts in question.

HOMELAND SECURITY ACT OF 2002 (HR5005), SEC. 102. SECRETARY [OF HOMELAND SECURITY]; FUNCTIONS.

(c) COORDINATION WITH NON-FEDERAL ENTITIES—With respect to homeland security, the Secretary shall coordinate through the Office of State and Local Coordination (established under section 801) (including the provision of training and equipment) with State and local government personnel, agencies, and authorities, with the private sector, and with other entities, including by—

(1) coordinating with State and local government personnel, agencies, and authorities, and with the private sector, to ensure adequate planning, equipment, training, and exercise activities;

(2) coordinating and, as appropriate, consolidating, the Federal Government's communications and systems of communications relating to homeland security with State and local government

personnel, agencies, and authorities, the private sector, other entities, and the public; and

(3) distributing or, as appropriate, coordinating the distribution of, warnings and information to State and local government personnel, agencies, and authorities and to the public.

HOMELAND SECURITY ACT OF 2002 (HR5005), Subtitle A—Coordination with Non-Federal Entities, SEC. 801. OFFICE FOR STATE AND LOCAL GOVERNMENT COORDINATION.

(a) ESTABLISHMENT—There is established within the Office of the Secretary the Office for State and Local Government Coordination, to oversee and coordinate departmental programs for and relationships with State and local governments.

(b) RESPONSIBILITIES—The Office established under subsection (a) shall—

(1) coordinate the activities of the Department relating to State and local government;

(2) assess, and advocate for, the resources needed by State and local government to implement the national strategy for combating terrorism;

(3) provide State and local government with regular information, research, and technical support to assist local efforts at securing the homeland; and

(4) develop a process for receiving meaningful input from State and local government to assist the development of the national strategy for combating terrorism and other homeland security activities.

HOMELAND SECURITY ACT OF 2002 (HR5005), SEC. 214. PROTECTION OF VOLUNTARILY SHARED CRITICAL INFRASTRUCTURE INFORMATION.

(a) PROTECTION—

(1) IN GENERAL—Notwithstanding any other provision of law, critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement specified in paragraph (2)—

(A) shall be exempt from disclosure under section 552 of title 5, United States Code (commonly referred to as the Freedom of Information Act);

(B) shall not be subject to any agency rules or judicial doctrine regarding ex parte communications with a decision making official;

(C) shall not, without the written consent of the person or entity submitting such information, be used directly by such agency, any other Federal, State, or local authority, or any third party, in any civil action arising under Federal or State law if such information is submitted in good faith;

(D) shall not, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or employee of the United States for purposes other than the purposes of this subtitle, except—

(i) in furtherance of an investigation or the prosecution of a criminal act; or

(ii) when disclosure of the information would be—

(I) to either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee thereof or subcommittee of any such joint committee; or

(II) to the Comptroller General, or any authorized representative of the Comptroller General, in the course of the performance of the duties of the General Accounting Office.

(E) shall not, if provided to a State or local government or government agency—

(i) be made available pursuant to any State or local law requiring disclosure of information or records;

(ii) otherwise be disclosed or distributed to any party by said State or local government or government agency without the written consent of the person or entity submitting such information; or

(iii) be used other than for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act; and

(F) does not constitute a waiver of any applicable privilege or protection provided under law, such as trade secret protection.

Appendix B. "Domestic Preparedness Checklist," National Governors Association, 2001 (excerpts)

- Review the state's emergency plan and make needed changes to correct any procedural problems encountered on September 11.

- Identify what intelligence information is needed at the state level, who can receive it, and assess security clearances with the Department of Defense and the FBI. Ensure governor has viable statutory mechanisms in place to share intelligence information between state and local agencies and consider mandating a formal communication network between the intelligence community and medical community.

- Examine state laws and authorities that relate to search and seizure, invasion of privacy, quarantine, evacuation, relocation or restricting access and consider enacting new health emergency powers act if necessary. (See Model State Emergency Health Powers Act.)

- Understand what the authorities and prohibitions are to using military assets in the state.

- Review current state laws dealing with record checks, background checks, and access to public records to ensure they do not interfere with security. Consider whether legislation changes in the state's

open records law are necessary to ensure the protection of sensitive documents; review information posted on websites concerning sensitive information and critical infrastructure protection.

- Review, update, and strengthen security procedures at potential terrorist targets in state including state capitol and state buildings.

- Review and update plan for continuity of government operations during emergencies.

- Review and update state evacuation plans.

- Develop an effective strategy for communicating the potential terrorism threat to the public and the media.

- Create a counterterrorism task force to identify shortfalls in legal authorities, programmatic authorities, and funding issues. Counterterrorism task forces should include Chief Information Officers and local capabilities, especially the EMTs, fire and rescue, public health and medical, public utilities, and disaster preparedness personnel whose responsibility it would be to respond to terrorist events.

- Take advantage of the Emergency Management Assistance Compact (EMAC). EMAC is an interstate mutual aid agreement that allows states to assist one another responding to all kinds of natural and man-mad disasters. EMAC offers a quick and easy way for states to send personnel and equipment to help disaster relief efforts in other states. A system like this enables experts to be used across jurisdictions and regions based on the nature of a particular event.

- Submit State Needs Assessments to Department of Justice. Over the last several years the Department of Justice has provided state and local jurisdictions with funds to assist in purchasing the specialized equipment required to respond to terrorist incidents effectively and safely. Currently, under congressional direction, the states, in order to receive these funds, are required to complete a state-wide threat and needs assessment and to provide the department a three-year comprehensive strategy addressing how these funds, and other department assistance, would be allocated within the state.

APPENDIX C. SECURITY GUIDELINES FOR THE ELECTRICITY SECTOR OVERVIEW—VERSION 1.0

These guidelines and their attachments describe general approaches, considerations, practices, and planning philosophies to be applied in protecting the electric infrastructure systems. Specific program or implementation of security considerations must reflect an individual organization's assessment of its own needs, vulnerabilities and consequences, and its tolerance for risk. Recognizing this, these guidelines do not represent any single or "cookbook" approach to electric sector infrastructure protection.

Presidential Decision Directive 63 (PDD-63), "Protecting America's Critical Infrastructures," officially identifies "electricity" as a critical infrastructure. PDD-63, and the later Homeland Security Presidential Directive–3 (HSPD-3) call for:

- A framework for cooperation within individual infrastructure sectors and with government for the vital mission of protecting critical infrastructures;

- The U.S. Department of Energy (DOE) to be the lead agency for the energy sectors; and,

- Sector coordinator functions and responsibilities. The DOE has designated the North America Electric Reliability Council (NERC) as the Sector Coordinator for the Electricity Sector (ES).

NERC, as the Sector Coordinator, has the responsibility to:

- Assess sector vulnerabilities,
- Develop a plan to reduce electric system vulnerabilities,
- Propose a system for identifying and averting attacks,
- Develop a plan to alert electricity sector participants and appropriate government agencies that an attack is imminent or in progress, and
- Assist in reconstituting minimum essential electric system capabilities in the aftermath of an attack.

The idea of protecting the electric system infrastructure is not new. The electric grid is designed to ensure a reliable supply of electricity, even in the face of adverse conditions. Throughout its history, the industry has been able to restore service consistently and quickly after earthquakes, hurricanes, major floods, ice storms, and a variety of other natural and manmade disasters. Its experience in emergency management has prepared the industry to respond effectively to a "spectrum of threats" using its existing structure, resources, and plans. This spectrum ranges from simple trespassing, to vandalism, to civil disturbances, to dedicated acts of terror and sabotage. Perpetrators include "insiders" and "outsiders" whose actions may be cyber or physical in nature.

In this context, it may be appropriate to periodically reevaluate existing plans, procedures, and protocols to consider vulnerabilities to a full spectrum of threats, particularly the unique aspects associated with terrorism.

These guidelines are meant to support those efforts. They are advisory in nature. Each company must assess their usefulness within the context of its operating environment and subject to its own evaluation of its vulnerability and risk to its perceived spectrum of threats.

These guidelines apply to "critical" operating assets. Each company is free to define and identify those facilities and functions it believes to be critical, keeping in mind that the ability to mitigate the loss of a facility

> For purposes of these guidelines, a critical facility may be defined as any facility or combination of facilities, if severely damaged or destroyed, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact to the reliability or operability of the energy grid, or would cause significant risk to public health and safety.

through redundancies may make that facility less critical than others. Each security guideline for the electricity sector is summarized below. Companies may wish to review their plans, practices, and procedures for these elements:

- **Vulnerability and Risk Assessment**
  Helps identify those facilities that may be critical to overall operations, as well as their vulnerabilities. Consideration should be given to closely safeguarding such information and restricting it to only a few individuals with a "need to know."

- **Threat Response Capability**
  Ensures that company personnel at critical operating facilities understand how to respond to a spectrum of threats, both physical and cyber. Consideration should be given to NERC's "Threat Alert Levels and Response Guidelines."

- **Emergency Management**
  Ensures that companies are prepared to respond to a spectrum of threats, both physical and cyber. Consideration should be given to reviewing, revising, and testing emergency plans on a regular basis. Plans might include training provisions for key responders to ensure they have the skills and knowledge to effectively carry out those plans.

  Maintaining comprehensive mutual assistance agreements at the local, state and regional levels also supports response, repair, and restoration activities in the event a critical facility is disrupted. Liaison relationships with local FBI offices as well as with other local law

enforcement agencies are also effective.

- **Continuity of Business Processes**
  Reduces the likelihood of prolonged interruptions and enhances prompt resumption of operations when interruptions occur. Consider flexible plans that address key areas such as telecommunications, information technology, customer service centers, facilities security, operations, generation, power delivery, customer remittance and payroll processes. It is useful to revise and test plans on a regular basis. It also is advisable to train personnel so they fully understand their roles with respect to the plans.

- **Communications**
  Ensures the effectiveness of threat response, emergency management, and business continuity plans. Consideration should be given to establishing liaison relationships with federal, state, county, and local law enforcement agencies in the area. Building the relationship might include providing tours of critical facilities for law enforcement agencies having jurisdiction in areas where those facilities are located, and planning to identify possible response needs. Such liaisons may need to be periodically updated and tested.

  Consideration also should be given to planning how personnel will respond to alarms, outages, or other issues at critical operating facilities. Robust communications systems such as radio, cellular phone, or similar communications devices are effective.

- **Physical Security**
  Mitigates the threat from inside and outside the organization. A Physical Security Program might include deterrence and prevention strategies. A systems approach is advisable, where detection, assessment, communication, and response are planned and supported by adequate policies, procedures, and resources.

- **Information Technology/Cyber Security**
  Mitigates the threat from inside and outside the organization. Consideration should be given to computer network monitoring and intrusion detection, placing particular attention on EMS, SCADA, or other key operating systems. It is advisable that only authorized persons have access to those critical systems, and only for valid pur-

poses. Consideration also should be given to adequate firewall protection and periodic audits of the network and existing security protocols. Third-party penetration testing may be useful.

- **Employment Screening**
  Mitigates the threat from inside the organization. Hiring standards and preemployment background investigations may help ensure the trustworthiness and reliability of personnel who have unescorted access to critical facilities, including contractors and vendors.

- **Protecting Potentially Sensitive Information**
  Reduces the likelihood that information could be used by those intending to damage critical facilities, disrupt operations, or harm individuals. Consider creating a hierarchical confidentiality classification framework (e.g., Public, Market Participant Confidential, Company Confidential, Highly Confidential) and the authorization requirements and conditions to permit disclosure.

Overall, training for new personnel and ongoing training for existing personnel on physical and cyber security policies, standards, and procedures are effective tools to mitigate threats.

Finally, each company must consider and comply with all applicable laws.

APPENDIX D. NASEO*
SUGGESTIONS TO ENHANCE ENERGY SECURITY AND IMPROVE FEDERAL AND STATE ENERGY EMERGENCY MITIGATION AND RESPONSE CAPABILITIES

February 10, 2003

It is vital that the states and the nation take steps to improve and enhance our ability to respond to energy emergencies. As the events of September 11 demonstrated, the nation remains vulnerable to international terrorism and the impacts that such events might have on our Nation's energy infrastructure. In addition, we continue to ponder the issue of increasing concern over the reliability of our electricity supply.

NASEO has a longstanding concern with energy emergency preparedness and response, which is described in *Issues 2000: NASEO's National Energy Issues Agenda* (see, Sustain the Strategic Petroleum Reserve and Strengthen Energy Emergency Preparedness[1]), a document that describes NASEO's views on the top issues priorities of the states. To assist both the U.S. Department of Energy (DOE) and the states and territories in strengthening energy emergency preparedness and response programs,

* The National Association of State Energy Officials (NASEO) is the national organization of the nation's state energy officials.

NASEO has developed the suggested program improvements and recommendations described below.

Improving What Works

NASEO suggests that any initiatives undertaken to improve our readiness to respond to energy emergencies should build upon and improve existing programs. The Energy Emergency Information Coordinators (EEIC) Program helps to provide information exchange, as do regional conference calls. The State Heating Oil and Propane Program (SHOPP) between EIA and the states provides valuable and timely information to both states and the federal government and is a good example of a cooperative program where the benefits far outweigh the costs. The State Energy Program (SEP), which has provisions that require states to have energy emergency plans, is an example of a program which, with proper guidance, can be used as a funding source for much of the state work that needs to be done.

The energy emergency-related provisions of the above efforts have helped the states and nation understand and react to energy emergency events. However, these initiatives have suffered from a number of reductions in resources, particularly in the area of state-federal cooperation and planning. NASEO believes that it is essential to strengthen the EEIC program and to develop and utilize a communications protocol between the Department, industry, and the states for use whenever the situation might be warranted.

We can build upon and improve our existing capability to meet the needs of our citizens in responding to energy emergencies. This can best be done through cooperative and joint efforts of the states, industry and DOE on behalf of the federal government. The following are specific recommendations, developed in conjunction with NASEO's Energy Data and Energy Security Committee, for areas that provide the best potential to improve existing programs and relationships.

1. The 1990 statutory revision of the State Energy Conservation Program included energy emergency planning as a mandatory feature (PL 101-440). NASEO believes that DOE should now assess the current status of states' and territories' energy emergency planning. This assessment should include information on the scope of the plans' coverage, energy sources covered, when plans were last updated, state agen-

cies involved in the plans and ongoing guidance. The results can be used to identify gaps and needs for emergency preparedness activities at both the state and federal levels.

2. DOE should work with states and territories to identify tools and specific contingency plans that can be used by states in energy emergencies to respond to specific conditions and circumstances. Actions such as driver hours' waivers, Jones Act waivers, temporary environmental waivers, and public information programs to encourage energy efficiency are all accepted responses to certain types of supply disruptions. However, relatively few states have taken action along these lines. Consequently, NASEO feels that our Energy Security Committee can develop model guidelines, which address plan components and provide examples of how to respond during prescribed circumstances. The Committee would also address policy options that are now available to states and have been tested most recently such as interruptible natural gas tariffs. In addition, we would guide states in developing plan elements that are sensitive to ongoing changes inherent in power market restructuring.

3. DOE, states, and industry representatives need to identify mitigation measures in the form of policies, tax incentives, voluntary measures or permanent regulatory changes that will improve the resiliency of the energy distribution system and enhance supply reliability. The assessment should identify critical infrastructure vulnerability for all forms of energy supply and delivery. In the heating fuels industry, for example, just-in-time delivery has reduced the cushion that protected customers from short-term supply disruptions. We must work together to examine creative measures to increase product inventories, whether through non-legislative or legislative means.

4. DOE should work with states to make operational the Energy Emergency Information Coordinator Program[2]. DOE should be the facilitator of regional cooperation and information during prescribed circumstances and distribute information to the states, including a select group of associations representing industry, in a timely manner. Likewise states (and industry participants) should readily share important information on their supply conditions with the DOE and surrounding jurisdictions.

5. DOE has indicated the need for States to work with their gas, electric and petroleum companies and the associations representing these companies to identify the vulnerability of critical infrastructure to terrorism. NASEO agrees and will work with the states to implement this request.

6. Regional energy emergency planning workshops should be developed to help states; DOE and others understand the workings of state plans. The actual number and location of such workshops would be responsive to national and state needs. An east coast and west coast workshop might be all that is necessary. The Department should discuss a number of different issues at the workshops and use a variety of techniques in order to encourage states to review and update their emergency plans, improve communications and their ability to assess energy market data in order to gauge an appropriate level of response. The workshops should encourage the use of DOE developed scenario analysis and simulations. Coordination of planning and building of relationships between states and with the federal government is an important component of the effort. These workshops should also be seen as evolutionary in nature, building from one year to the next. The workshops should be seen as a tool for training, education and enhancing preparedness. If the workshops were held in a multi-year repeating cycle, they could be conducted on a regional or national basis. The multi-year cycle could include a few common elements each year, such as updated threat assessments or vulnerability analyses. Ideally, we should work to ensure that appropriate participants from each state and territory energy office participate in the workshops[3].

Notes

1. See: http://www.naseo.org/issues/issues_agenda.htm.

2. See: http://www.naseo.org/tforces/energyinfo/emergency.htm.

3. For example, a three-year workshop cycle could include the following items: Year 1: Regional workshops focusing on state energy emergency plans and plan development. Year 2: A National workshop focusing on communications and coordination within and among states, DOE, and industry. Year 3: Regional workshops devoted to energy emergency exercises. It is critical that these workshops have the active involvement of the private sector in both the planning and participation stages.

Appendix E. Critical Energy Infrastructure Protection Reports and Studies, NASEO Energy Data Committee, 2001

The National Strategy For Homeland Security: (July 2002) Office of Homeland Security
http://www.whitehouse.gov/homeland/book/index.html

U.S. Should Harness Science and Technology Capabilities to Fight Terrorism (2002)—National Research Council Division on Engineering and Physical Sciences
http://www.nap.edu/books/0309084814/html/

Critical Infrastructure Protection: Significant Challenges Need to be Addressed—General Accounting Office. (July 24, 2002)
http://www.gao.gov/new.items/d02961t.pdf

Reports on State Homeland Security Structures— The National Emergency Management Association (NEMA) and The Council of State Governments recently conducted a joint survey of the 50 states and District of Columbia to determine the organizational structure of each state to address terrorism preparedness. (2002)
http://www.nemaweb.org/News/NEMA_Homeland_Security_Report.pdf

Task Force on Protecting Democracy—National Conference of State Legislatures' (NCSL). (July 25, 2002)
http://www.ncsl.org/programs/press/2002/pr020725protect.htm

Emergency Planning and Preparedness: Securing Oil and Natural Gas Infrastructures In the New Economy (June 6, 2001)—National Petroleum Council
http://www.securitymanagement.com/library/NPC_Tech0901.pdf

National Energy Security Post 9/11— The United States Energy Association (USEA) . The report reflects the efforts of USEA members to summarize our core principles and present broad policy recommendations with regards to the security of the energy sector. (July 19, 2002) For a copy of the report see:
http://www.usea.org/USEAReport.pdf

Task Force on Electricity Infrastructure — The National Governor's Association (NGA), has released a report that recommends the creation of Multi-State Entities (MSEs) to facilitate state coordination on transmission planning, certification, and siting at a regional level. (2002)
http://www.nga.org/cda/files/INTERSTATESTRATEGIES PLANNING.pdf

Testimony on The Nation's Energy Infrastructure—Pat Wood, III Chairman, Federal Energy Regulatory Commission Before the Senate Committee on Energy and Natural Resources United States. (July 24, 2002)
http://www.ferc.gov/news/congressionaltestimony/WoodTestimony 07-24-02.pdf

Notes

Chapter 2

1. "The Cost of Power Disturbances to Industrial and Digital Economy Companies," June 2001, Madison Wisconsin. By Primen, for the Consortium for Electric Infrastructure to Support a Digital Society, an Initiative by EPRI and the Electricity Innovation Institute (E2I).

Chapter 3

1. Julie Offner, Nuclear Energy Institute, personal communication with author, 2003.

2. *Nuclear Security—Before and After September 11*, U.S. Nuclear Regulatory Commission, http://www.nrc.gov/what-we-do/safeguards/response-911.html.

3. *Nuclear Power Plant Emergency*, Feb. 11, 2003, FEMA Hazards Backgrounder. http://www.fema.gov/hazards/nuclear/radiolo.shtm.

4. "Albany Says it Can't Certify Indian Point Evacuation Plan," *The New York Times*, Jan. 31, 2003.

5. The NRC issues certificates for radioactive materials packaging, including spent fuel casks, that verify compliance with safety standards. The certification essentially means that the cask will withstand severe transportation accidents with minimal chance of release of its contents. The NRC, the main/major enforcer of DOT radioactive materials regulations, has the lead role in investigating accidents that involve NRC-

certified packages. NRC also requires advance notification to state governors of spent fuel shipments and enforces requirements for safeguarding shipments.

6. The DOE must comply with all DOT and NRC transportation regulations and has stated that it will comply with all applicable state requirements that are not preempted by federal law. Under the Nuclear Waste Policy Act, DOE will take title to spent fuel at the reactor, provide casks for transport, arrange for shipments, manage its transportation contractors, assist state and local governments to respond to transportation emergencies, and provide technical and financial assistance to states and Indian tribes for emergency response training.

7. LNG remains a relatively small component of total gas storage. Most natural gas is stored in underground caverns.

8. Energy Information Administration, 2002.

9. Energy Information Administration, 2002.

10. "U.S. Refiners Face Security, Supply Issues: ConocoPhillips," *Platt's Global Alert,* March 25, 2003.

11. Committee on Critical Infrastructure Protection, National Petroleum Council. *Securing Oil and Natural Gas Infrastructure in the New Economy,* June 2001, National Petroleum Council, 5.

12. Ibid.

13. Ibid.

Chapter 5

1. President Bush's Executive Summary on Homeland Security discusses these new roles (available at http://www.whitehouse.gov/deptofhomeland/sect1.html).

Chapter 6

1. Most respondents indicated that they offer FOIA protection for sensitive utility security information, while 22 percent indicated they did not. The majority of survey respondents also indicated that protective orders for confidential information would dispel the utilities' concerns.

2. Office of Homeland Security, *National Strategy for Homeland Security*, July 2002, p. 57.

3. Richard Forno, "Information Resilience and Homeland Security," *Security Focus Online*, May 9, 2002, http://online.security focus.com/columnists/80.

4. Homeland Security Act of 2002, Section 214 (a) (1) (c).

5. Ibid., Section 214 (a) (1) (E) (iii).

Chapter 7

1. Robert E. Burns, John Wilhelm and Ted Lehmann, *State Commission Regulatory Considerations Concerning Security-Related Cost Recovery in Utility Network Industries* (Columbus, Ohio: National Regulatory Research Institute, November 2002.

2. Ibid.

3. Utilities and commissions may initiate more rate cases in the coming few years. The infrequency of rate cases in the 1990s may have been an unusual phenomenon.

Chapter 8

1. NARUC Ad Hoc Committee on Critical Infrastructure, *Discussion Draft Paper on State Government Organizational Issues*, March 14, 2003.

Chapter 9

1. This is one area in which hours of service restrictions on driver's licenses may be critical to energy providers.

2. During the 1980s and 1990s and in the year 2000, the U.S. DOE sponsored regional emergency-management exercises. State energy officials remember these exercises as useful methods of gaining experience and developing relationships with colleagues in other states.

3. http://www.naseo.org/eeic/contacts.htm.

Chapter 14

1. Connecticut, Sec. 16-50g.

Chapter 15

1. "Smaller, Closer Dirtier: Diesel Backup Generators in California," *Environmental Defense* (2002), 5.

Chapter 16

1. California has attempted to regulate vehicle fuel efficiency through an indirect method: limiting vehicle carbon dioxide emissions. Although under challenge from a number of sources, 2002 California law requires the state to develop vehicle carbon emissions limits. The only practical way to reduce vehicle carbon emissions is by increasing vehicle fuel efficiency.

Chapter 17

1. NARUC Ad Hoc Committee on Critical Infrastructure, *Discussion Draft Paper on State Government Organizational Issues*, March 14, 2003.

2. The Pacific Northwest Economic Region (PNWER), U.S. Navy, Federal Emergency Management Agency, and Canadian Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP)

coordinated a multi-jurisdiction, cross-border tabletop exercise on infrastructure interdependencies in June 2002.