

8. PROTECTING ENERGY INFRASTRUCTURE

Electricity and transportation fuels are essential to the American way of life. Today, their vulnerability to disruption calls for a better strategy for securing energy infrastructure. Disruptive incidents occur fairly frequently, but rarely cause significant harm because disruptions tend to be localized, whereas infrastructure is redundant, geographically dispersed, and supported by facility owners experienced in repair and service restoration. Nevertheless, America's infrastructure for electricity and transportation fuels is susceptible to damage—natural, accidental, or intentional—that could have devastating consequences.

While the consequences of energy infrastructure failures can be severe, these are low-probability events and there are specific steps that can reduce their likelihood and consequences. Fortunately, most infrastructure is not critical: Of the vast network of pipelines, pumping stations, refineries and other facilities, few would fall into the category of “essential systems,” the loss of which would significantly harm large segments of the economy or the population; even fewer would be appropriately classified as “high-impact targets.”

These characteristics suggest a three-part risk management strategy for securing energy infrastructure:

- ◆ eliminate, or, if that is not feasible, heavily guard energy assets that can be used to injure or kill large numbers of people;
- ◆ invest in redundancy to prevent any single failure from bringing down large parts of the national energy system; and
- ◆ make systems resilient so that, when they do fail, the system can be restored quickly.

This chapter will survey the security issues and vulnerabilities relevant to the most important categories of the energy infrastructure, review

current protective measures, and propose ways to remedy vulnerabilities. It will close with recommendations to reduce the nation's vulnerability to energy infrastructure failure in the future.

INFRASTRUCTURE PROTECTION AS RISK MANAGEMENT

Securing energy infrastructure is fundamentally a risk management exercise, where risk is defined as a function of threat (intent and capabilities of adversaries), vulnerabilities (security and design weaknesses), and consequences (potential adverse effects). Given an understanding of the threats, vulnerabilities, and consequences, security and asset managers can design and implement prevention and remediation programs that make sense.

THREAT ASSESSMENT

The record of the last decade suggests that jihadists possess both the intent and the capability to strike at U.S.-based energy assets and systems. The 2002 attack on the French supertanker *Limburg* showed that al Qaeda is attuned to the energy industry and able to stage attacks of impressive sophistication. In Iraq, insurgents have persistently and successfully attacked energy infrastructure. Jihadists employed these skills, albeit unsuccessfully, in a February 24, 2006, attack against the Abqaiq oil facility in Saudi Arabia. It is clear that jihadist groups have the capability to strike our energy infrastructure and that these attacks against energy assets could fulfill their goal of killing large numbers of Americans and crippling our economy.

Of course, terrorism is not the only threat to the energy sector. Natural disasters, such as earthquakes or hurricanes, can damage or destroy electric transmission lines and transformers, gas pipelines, hydroelectric dams, or coal-carrying trains and tracks. A six-day ice storm that swept Quebec, Ontario, New Brunswick, and Maine in 1998 damaged so much transmission and distribution equipment that

over 4.5 million people were left without power. Some of the damage took months to repair. The hurricanes of fall 2005 halted oil and gas flow from the Gulf of Mexico for almost a week, having shut down or damaged refineries, off-shore production platforms, and pipelines across the Gulf.

Human error can be equally damaging. On August 14, 2003, a series of individually small computer software and hardware failures, combined with operator inattention, led to a blackout that cut service to over 50 million people in the United States and Canada. Every major U.S. electrical blackout since 1965 has occurred in part due to human error (misspecification of equipment, faulty maintenance practices, or misjudged tolerances) that led to system failure under stress. The same is true of many accidents at dams and refineries.

VULNERABILITY ASSESSMENT

Energy infrastructure is vulnerable to a range of hazards:

- ◆ natural disasters (hurricanes, earthquakes, floods, landslides, ice storms, and forest fires);
- ◆ unintentional human-caused damage (construction equipment cutting gas pipelines, vehicles striking distribution poles, bad software, and so forth);
- ◆ malicious attacks by individuals (disgruntled employees sabotaging equipment, drunks firing at pipelines);
- ◆ coordinated terrorist attacks (armed attack on a nuclear power plant or large dam, use of explosives to damage multiple pipeline facilities, substations, or refineries);
- ◆ cyber attack (dissemination of viruses, denial-of-service attacks against control systems, probes that take over or feed false information to a control system); and
- ◆ loss of other parallel infrastructures, on which energy operations depend (including telecommunications, the Internet, banking, transportation, fuel deliveries—coal via railroad or gas via pipeline—or water supplies).

CONSEQUENCE ASSESSMENT

Four primary factors determine whether an energy system failure has either localized or major social consequences.

- ◆ First, the magnitude and speed of the asset failures. Phenomena such as hurricanes, ice storms, and earthquakes damage multiple facilities across large geographic areas, thereby compromising much of the system simultaneously. Service to millions of customers may be affected and system restoration and recovery can be a slow, asset-by-asset rebuilding process.
- ◆ Second, the impact of initial failure on interrelated systems. Electricity systems are particularly vulnerable to cascading failure—that is, where the failure of one element triggers failure in successive elements—because they are heavily computerized, thoroughly interconnected, and react with split-second speed to failures elsewhere in the system. In contrast, infrastructures that move physical commodities such as oil, natural gas, petroleum products, and coal can sustain significant physical damage in a few locations without collapse of the overall system.
- ◆ Third, the extent of the damage and the speed with which service can be restored. In most cases, the failure of a single asset will not compromise system performance for long, if at all; the exception is a supervisory control and data acquisition (SCADA) system, a centralized monitoring and control system for transport. However, if multiple assets within a system fail simultaneously, the overall system is much more likely to fail.
- ◆ Fourth, the length of time that critical infrastructures are unavailable. In most energy infrastructures, managers can circumvent the loss of a few critical assets and still keep the system working. However, the longer the critical assets are unavailable, the more difficult it becomes to sustain system performance. A metropolitan area can tolerate a blackout for several hours or even a day, but if it lasts much longer, it can trigger failures of telecommunications, traffic, water, sewer, and public safety. An energy system failure caused by the simultaneous destruction of multiple critical assets would cause a lengthy service interruption, and have a traumatic effect on the people and economy of the region.

SECURITY OF ENERGY ASSETS

Each energy asset has a set of unique associated threats, risks, and consequences, which dictate the appropriate set of security measures. Two considerations are central: whether the asset can be protected at all, and the implications of failure for the system as a whole.

Many energy assets can fail without significantly affecting the performance of the larger energy delivery system. The catastrophic failure of an individual asset such as a power plant, dam, pipeline, oil refinery, or liquefied natural gas (LNG) terminal could have disastrous consequences for those who live and work around the facility, but would not necessarily compromise the performance of the entire energy system. The same is true for facility attacks, such as an airplane crashing into a nuclear power plant or a refinery bombing. These attacks could have great symbolic and socially traumatic effects without disrupting system function.

FOSSIL AND NON-NUCLEAR POWER PLANTS

There are approximately 16,770 generators in the United States with a total capacity of 1,049,615 megawatts (one megawatt serves about 800 homes).¹ These generators use diverse fuel sources—32 percent of the capacity is coal-fired, 4 percent oil, 18 percent natural gas, 18 percent dual-fired (oil and gas), 10 percent nuclear, 9 percent hydroelectric, and approximately 2 percent renewable.

Individual plants are commonly taken off-line for maintenance, or because there are times when plant operation is uneconomical. Grid operators are therefore accustomed to juggling planned and unplanned generation outages without compromising system reliability. Thus, in most cases, the sudden loss of the output from one or two power plants due to coordinated attack or a widespread natural disaster would not compromise the ability of the overall electric system to continue producing and delivering electricity.

However, the location of the affected generator matters a great deal. Certain plants, by nature of their place within the grid, provide

important reliability services that cannot easily be replaced by a generator located elsewhere. If such a plant were incapacitated at a time of high electric use, the resulting grid imbalance could lead to a wider system imbalance and a local blackout.

A successful attack against a non-nuclear power plant or its on-site fuel supplies is not inconceivable. Although these facilities have large security perimeters, they are accorded only moderate physical protection and limited monitoring. Most of the damage from a major attack on such a plant would be contained within its perimeter, and would be unlikely to cause catastrophic damage beyond the site of the plant itself.

NUCLEAR POWER PLANTS

There are 103 operating commercial nuclear power plants at 65 sites across the United States, providing 10 percent of the nation's electricity production. Although the power plant is the primary focus of concern, security of adjoining spent fuel storage cannot be ignored. Blast and fire damage from a nuclear power plant accident or attack would likely be contained within the plant property.

An incident of this kind could also result in a radioactive release, drifting in an airborne plume from the targeted facility for miles into the surrounding area. Such a release could afflict between 50,000 and 500,000 people in nearby and downwind areas with radiation burns, immediate and long-term cancers, and other health problems. The health effects of a nuclear accident or attack would obviously depend largely on the location of the nuclear source relative to population centers.

The fact is that many nuclear plants are close to major metropolitan areas, including New York City, Boston, Philadelphia, and New Orleans. Consequences of a radioactive release might include the need to permanently relocate entire communities at extraordinary economic, social, and emotional cost. Essential safety measures at nuclear plants include reactor containment buildings designed to protect the reactor against damage from hurricanes, tornadoes, and terrorist attacks (as well as to contain possible radiation releases). Nuclear plants have a variety of automated safety mechanisms that should shut down the plant in the event of an attack or internal failure.

The Nuclear Regulatory Commission (NRC) requires every nuclear licensee to perform a variety of detailed security analyses, implement emergency preparation plans and exercise them in concert with the local community, and provide additional safety and security training for all plant and guard personnel. Since 2001, every nuclear power plant has established concentric security zones around the plant core, and enhanced its physical protection features and defenses with fences, barriers, cameras, and patrols by armed guards. Nuclear plants conduct “force-on-force” exercises and a variety of inspections to test guard and plant readiness. Access to the airspace above nuclear plants and the navigable waters next to them is strictly limited.

There is continuing public debate over whether nuclear power plants are as safe and secure as industry and federal regulators claim. Some of the points of contention revolve around whether the plants, designed and built in the 1970s, can stand up to modern methods of attack—for instance, whether a reactor containment vessel can withstand a direct hit from a large aircraft. The NRC tests plant security and designs against a “design basis threat,” which specifies the assumed maximum assault or potential failure mode that the plant could face, and then analyzes the plant’s ability to withstand that threat. Organizations such as the Union of Concerned Scientists maintain that the NRC’s safety and security requirements are inadequate. A National Academy of Sciences study concluded that cutting the water supply to a nuclear power plant’s spent nuclear fuel pool could lead to a high-temperature radiation fire that could release as much radiation and cause as much death and disease as a meltdown within the plant’s nuclear core.² On the other hand, the Nuclear Education Institute claims that a successful attack on a nuclear power plant would require many experts, and that reactors are so heavily protected that terrorists will probably choose to attack easier targets instead.

HYDROELECTRIC DAMS

Within the United States, there are over 5,500 large dams. Over one-third of them are owned by utilities to produce electricity. These dams are sited and licensed by the Federal Energy Regulatory Commission

(FERC). Most other large dams are owned and operated by federal government agencies, primarily the Bureau of Reclamation and the Army Corps of Engineers, for multiple uses including power production, flood control, transportation, irrigation, and public recreation. Hydroelectricity from private and federal dams contributed 7 percent of the nation's total electricity consumption in 2004.

Some large dams, like the Hoover and Grand Coulee dams, have great symbolic value. A successful attack on such a facility would affect the nation's psyche far more than it would the electric grid. For most dams, the consequence of greatest concern is that a sudden dam rupture could result in an uncontrolled water release that would harm people and property downstream. The Federal Emergency Management Agency (FEMA) has identified more than 10,000 dams as having "high hazard potential," meaning that their failure from any means, including a terrorist attack, could result in significant property damage, environmental damage, and loss of life.

Dam owners and operators have worked with the three federal agencies (FERC, Bureau of Reclamation, and the Army Corps) to develop and implement risk assessment methodology and safety and security practices designed specifically for dams. Since 2001, all dams used for electricity production have made extensive security improvements, such as installing new sensors, barriers, and communications equipment. FERC safety inspectors conduct regular security audits of their jurisdictional dams and require dam owners to develop and practice emergency action plans. Under the Dam Safety and Security Act of 2002, FEMA is the designated federal coordinator for dam safety and security—yet another reason to restore the capacities of FEMA that were undermined through its incorporation into DHS.

ELECTRICITY SYSTEM

The U.S. electric system is a web of power plants linked to customers by 163,000 miles of high-voltage transmission lines, distribution lines, and supporting equipment. U.S. electricity demand for the summer of 2006 is expected to reach 744,000 megawatts, served by almost 890,000 megawatts of generation resources—19.5 percent over demand.³

While this surplus capacity suggests that the electrical grid can survive the loss of multiple assets without failing, some assets, as noted above, are more important than others, and the simultaneous loss of too many physical or cyber assets could lead to cascading failure and black-outs over a large part of the grid.

Computer-automated controls and communications manage the entire electric grid, and a failure in one asset-owner's supervisory control and data acquisition (SCADA) system can cascade instantly across the entire grid. This makes cyber security a critical necessity for the electric industry, which has been developing and refining voluntary cyber security standards since 2002.⁴ Those standards became mandatory for industry members in 2006, when the Federal Energy Regulatory Commission assumed regulatory responsibility for electric reliability under the Energy Policy Act of 2005.

The Federal Bureau of Investigation recently asserted that terrorist groups such as al Qaeda do not have the ability to disable power plants and other critical infrastructure through the Internet. FBI officials state that they are not aware of any terrorist plans to attack U.S. infrastructure, but that many intrusion cases appear to be sponsored by foreign nations.⁵ A survey of utility information technology executives in summer 2005 found that 20 percent reported that their SCADA systems have already been probed by outside threats, and one-third expect that the SCADA or energy distribution systems of at least one utility company will be attacked or compromised during the next two years.⁶

The transmission network faces operational issues, including congestion and steadily rising electricity flows across the grid. For a decade, utilities underinvested in transmission, and are only now building major new facilities to strengthen grid performance, delivery throughput, and reliability. Because the majority of power plants are located far from the large urban areas where most electricity is used, and because many regions of the country import low-cost generation from other regions, an adequate transmission grid is crucial to maintaining service.

Several problems can disrupt transmission system performance: inadequate capacity, as suggested earlier; failure to prevent trees from growing into and shorting out power lines; and the very nature of custom-designed transformers or breakers that are hard to replace when they break. Transmission lines themselves are very long, highly visible, and impossible to hide or protect, and therefore vulnerable to the havoc wrought by nature or terrorist attack.

OIL AND GAS PRODUCTION FACILITIES

Oil and natural gas provide 60 percent of the United States's energy needs and serve as raw materials for the manufacture of plastics, chemicals, fertilizer, medicines, and synthetic fibers. In 2004 the nation consumed 20.7 million barrels of oil per day, and imported 58 percent of that amount from five countries: Canada, Mexico, Saudi Arabia, Venezuela, and Nigeria. Domestic oil production came from over half a million oil wells, with a quarter of production from offshore, primarily deep-water wells in the Gulf of Mexico.⁷ The United States also consumed 22,375 billion cubic feet of natural gas in 2003, 82 percent of which came from domestic wells.⁸

Although most domestic oil and gas wells are individually small and dispersed, they are concentrated within particular geographic regions, making it easier and potentially more disruptive should terrorists disable oil and gas gathering systems rather than individual wells or fields. This was illustrated by Hurricanes Katrina and Rita, which together shut down all oil and gas production from the Gulf of Mexico for at least a week. Four months later, only three-fourths of that production had been restored. The hurricanes destroyed many deep-water drilling rigs and damaged others. Although many onshore pipelines were not harmed, over 5.25 billion cubic feet of daily gas processing plant capacity was damaged and took months to rebuild.

Over the short term, the net result of the damage restricted supplies of natural gas to much of the southern United States. Natural gas prices jumped immediately and, combined with curtailed supplies from the Gulf, prices remained at record high levels for months.

OIL REFINERIES

There were 144 refineries operating in the United States at the start of 2003, processing over 17 million barrels of oil per day.⁹ Most are in the Southeast, along the Gulf Coast. No new oil refinery capacity has been built in the United States since 1976, although refinery owners have steadily worked to improve efficiency and plant reliability. However, with domestic demand for finished petroleum products increasing every year,

United States imports from the Caribbean, Venezuela, and Europe have increased to over 2 million barrels of gasoline per day.

The March 2005 explosion of British Petroleum's Houston refinery was a harsh example of the consequences of an accident, with 15 people dead and over 100 injured. While the physical destruction from a refinery explosion may be contained within the facility perimeter, many refineries use a variety of hazardous chemicals that can threaten adjoining communities. One such chemical is hydrofluoric acid, which as an aerosol will burn human tissue.

The use of these chemicals would be subject to the proposed Chemical Facility Anti-Terrorism Act of 2005, which could increase costs enough to force companies to switch to less dangerous processes. If this act does not pass, other means should be explored to eliminate this danger.

Because of the high level of environmental and physical damage that could result from a refinery explosion and refineries' high capital cost, refineries are closely guarded facilities. Most are closely monitored and have extensive buffer zones and robust physical protection. Refinery owners have worked with the Department of Homeland Security, the Coast Guard, and federal intelligence and law enforcement agencies on security assessments, emergency operation plans, and information sharing about threats and best security practices.

OIL AND GAS PIPELINES

There are over 2 million miles of oil and gas pipelines in the United States. Pipelines transport two-thirds of the oil we consume.¹⁰ Most pipelines are buried at least a meter underground; but some stretches, as well as associated facilities such as pumping stations and tank farms, are above ground.

Almost 190 billion cubic feet per day of natural gas moved through interstate and intrastate gas transmission pipelines in 2004. Much of this gas flows either from Texas and Louisiana (onshore or in the Gulf of Mexico) to the Southeast or Southwest, from the Rockies westward or toward the Midwest, and from Canada southward into the Pacific Northwest and California, into the Midwest, or into New England.

Pipeline investment has grown with natural gas demand, with total mileage increasing by about 1 percent per year and system capacity increasing by 4 percent annually with improved transport and storage practices. Underground natural gas storage facilities supplement the pipeline system by allowing a gas provider to keep a local inventory to help meet demands that exceed pipeline delivery capacity.

Since 1990, there have been nearly 2,300 major natural gas pipeline accidents resulting in over 200 deaths. Most of the accidents were at the local distribution company level (affecting smaller pipelines carrying gas within a metropolitan area), due to “outside forces” such as damage by the pipeline owner, third-party damage (as by contractor dig-ins), and natural disasters such as landslides and fires. There have been very few attacks (crime, vandalism, sabotage, or terrorist attack) upon U.S. oil or gas pipelines. Another principal cause of pipeline failure is pipe corrosion, which leads to a rupture and fuel spill, in the case of oil, or explosion, in the case of gas. However, corrosion protection and leak detection programs have significantly improved pipeline safety.

LIQUEFIED NATURAL GAS TERMINALS

Liquefied natural gas (LNG) is methane that has been cooled to -260° F, which condenses the gas and allows for storage and transportation in tanker trucks or ships. The United States has 108 working LNG facilities including six active LNG terminals (in Louisiana, Georgia, Massachusetts, Maryland, Alaska, and Puerto Rico). At present, LNG deliveries account for only 2–3 percent of U.S. gas imports, but, with high natural gas prices and growing demand, another twelve terminals have been approved for construction (five in Texas, three in Louisiana, two in the Bahamas, and one in Massachusetts), with many more proposed. There are 150 LNG tankers worldwide, with another fifty-five on order or under construction. LNG deliveries into the United States will increase markedly as new LNG receiving terminals go into service.

Since LNG maritime transport began in 1959, there have been only eight significant tanker incidents in over 33,000 tanker voyages, and no hull failures or cargo tank ruptures. The most significant LNG facility

accident was in 1944, when a gas tank rupture in Cleveland released gas that ignited in a residential neighborhood, killing 128 people and injuring many more. In 1977, a valve failure in Arzew, Algeria, released gas that froze one worker, although the gas did not ignite. In 1979, a gas leak at the Cove Point, Maryland, LNG terminal ignited within an electrical substation, leading to two deaths and extensive property damage. A fourth gas-related accident occurred in 2004 in Skikda, Algeria, where an explosion killed twenty-seven workers and injured seventy-two others; investigation, however, has not established whether this was caused by an LNG leak.

LNG is a homeland security concern because the potential consequences of an LNG accident or attack could be profound. LNG is not explosive, but when it is released into open air it warms and forms a vapor pool. At the edges of the pool, a 5 to 15 percent mixture of gas to air will ignite if exposed to flame or sparks and will burn at very high temperatures until the supply of gas is exhausted. This floating vapor pool expands as the supply of gas from a leak or tank rupture continues, and can be carried or pushed for up to a mile by the wind. The heat from such a fire is high enough to ignite wood, damage metal, and cause first- or second-degree burns to humans as far as one mile from the initial release site. While there is general agreement on the dangers of LNG, there is some dispute about the details because most LNG damage estimates are based on engineering analyses rather than observation and measurement of actual, large-scale LNG incident results.

The destructive potential of an attack on LNG tankers or onshore facilities makes them potential targets for terrorists. Several methods of attack seem plausible:

- ◆ attack a tanker to release and burn its cargo;
- ◆ use a tanker to aim a vapor pool fire at an onshore target;
- ◆ direct a tanker at an onshore target and then burn its cargo;
- ◆ use explosive weapons against a moving or docked tanker;
- ◆ run an explosives-laden boat into a tanker;
- ◆ sabotage an LNG plant or vessel through a worker or crew member; or
- ◆ load a car or truck with explosives and penetrate and damage an LNG facility.

The Department of Homeland Security and others regard LNG facilities as likely targets for terrorist attack for good reasons.

Because of these risks and the very hazardous consequences of a potential LNG incident, LNG terminals and tankers use extensive security measures. The location of LNG terminals is regulated by the Federal Energy Regulatory Commission (FERC). The FERC, the Coast Guard, and the Department of Transportation regulate and inspect facility safety and security. LNG terminal safety features include spill containment; fire-protection systems; gas, flame, smoke, and temperature detection and alarm systems; automatic and manual shut-down controls; and a barrier-enclosed security perimeter.

For LNG tankers, design and construction standards were established by the International Maritime Organization and upgraded by the Maritime Transportation Security Act of 2002. The U.S. Coast Guard requires tankers to follow strict security procedures as they approach and enter a port, including ninety-two-hour advance notification before arrival, harbor escort by marshals, limited port and airspace traffic to prevent collisions, on-board inspections, and verification of crew member identities.

Despite these precautions, LNG tankers and terminals remain a high-impact target, attractive to those intent on killing large numbers of people. The number of import terminals in the United States is set to increase, but government policy can help prevent or limit their development in densely populated areas. Our best defense is to deny our adversaries these deadly opportunities.

RECOMMENDATIONS

The federal government has a critical role in reducing the probability of the catastrophic failure of the nation's energy infrastructure. Policy measures are needed to:

8.1. RELOCATE THE MOST VULNERABLE ASSETS, SUCH AS LNG TERMINALS, AWAY FROM POPULATION CENTERS. Where this is not feasible, mandate increased security measures.

8.2. INCREASE THE REDUNDANCY OF OUR ENERGY INFRASTRUCTURE TO REDUCE VULNERABILITY. Redundancy entails creating both extra capacity within the network and backup capability to be used if part of the network fails. The latter is expensive but the former can increase system efficiency without significantly increasing the cost of delivered energy.

8.3. INCREASE SYSTEM RESILIENCY AND RECOVERY SPEED. Federal assistance for nationally critical investments can improve system resiliency and service restoration speed. Measures that improve recovery include careful planning and practice, maintaining inventories of parts that require a long lead time to replace, and effective relationship building and communications before and after the emergency.

8.4. STRENGTHEN OTHER INFRASTRUCTURES AND SYSTEMS, THOSE THAT BOTH SUPPORT AND DEPEND ON ENERGY SYSTEMS. A region with effective first responders, acute care capabilities, and backup power supplies for telecommunications, sewage, and water will be better prepared for energy system failures. In the long run, it is more cost effective to prepare for worst case outcomes than to respond to failures.

8.5. FOCUS ON ENERGY SECURITY, THAT IS, THE LONG-TERM AVAILABILITY OF RELIABLE, AFFORDABLE ENERGY SUPPLIES TO THE NATION. Because much of America's critical petroleum infrastructure is overseas, our oil and natural gas imports (with the exception of those from Canada and Mexico) must arrive by tanker, through maritime chokepoints like the Strait of Hormuz (at the entrance to the Persian Gulf), the Panama and Suez canals, and the Strait of Malacca (linking the Indian and Pacific Oceans).

Sudden increases in energy price levels can have dramatic consequences on domestic manufacturing competitiveness and in human social and physical comfort levels, as illustrated by the oil price shock of 1973 and the natural gas and gasoline price shocks of 2005. The United States should take proactive steps to reduce energy imports by making our vehicles, buildings, and business processes more energy-efficient. We must also invest more in wind, solar, and biomass technologies—especially near urban centers and critical security assets that face attacks on

conventional energy facilities. The federal government must use grants and tax incentives to expand and diversify our energy portfolio and reduce the need for long-distance fuel transportation.

8.6. INCREASE THE USE OF SMALL-SCALE DISTRIBUTED GENERATION (INCLUDING RENEWABLES AND COMBINED HEAT AND POWER) CLOSE TO ENERGY USERS. This would reduce our dependence on large-scale power plants and long-distance transmission lines, which are more inviting targets for attack and have greater consequences when they fail. Distributed generation is particularly needed to support other critical infrastructures such as telecommunications, sewage, and water, as well as to support natural gas and petroleum pipeline operations, so these infrastructures can continue operating in the event of a power outage.

8.7. INCREASE INVESTMENT IN RESEARCH, DEVELOPMENT, AND DEPLOYMENT OF DESIGNS THAT WILL MAKE ENERGY INFRASTRUCTURES AND NETWORKS MORE RESILIENT AND RESISTANT TO FAILURE.



Given the critical role of energy in supporting our economy and our way of life, our nation needs to invest significantly more attention, priority, and money to make our energy infrastructure and sources more reliable and secure. These investments will cause modest increases in the short-term cost of energy, but the long-term benefits of more reliable and secure energy systems are surely worth it.