Nuclear Energy and Terrorism

Paul Gaukler, D. Sean Barnett, and Douglas J. Rosinski

Since the terrorist attacks of September 11, 2001, concerns have been voiced that one of the nation's 103 commercial nuclear power plants might be the next terrorist target. Immediately following the attack, the Nuclear Regulatory Commission (NRC or Commission) ordered a heightened state of alert at all nuclear plants. Calls went out to augment nuclear plant security forces and some governors deployed National Guard troops at nuclear facilities. The U.S. House of Representatives passed legislation (H.R. 2983) that could drastically revise the Commission's security requirements for nuclear facilities. A proposed Senate bill (S. 1746) would federalize nuclear plant security forces. Additionally, there have been calls for installing anti-aircraft weapons at nuclear plants and creating permanent "no fly" zones around them. Some nuclear power opponents, claiming that nuclear plants are highly vulnerable to terrorist attacks, have seized on the events of September 11 as their latest argument for shutting down the nation's nuclear industry.

The public is understandably sensitive to nuclear plant safety issues in light of September 11 and some fear that nuclear plants will be attractive targets for terrorists. However, commercial nuclear plants are probably the most physically secure and least vulnerable of our nation's industrial infrastructure. They are robust, hardened facilities with numerous redundant systems designed to assure public safety, and are subject to close regulation by the NRC. Comprehensive NRC security requirements, including physical protection systems, armed guards, and strict access controls, are mandated for all nuclear plants.

This article explores the vulnerability of nuclear power plants to acts of terrorism. We describe the physical, security, and emergency response requirements applicable to nuclear plants and consider whether NRC security requirements can serve as a model for improving security at other infrastructure as well. We also explore policy issues concerning the appropriate division of responsibility between industrial security and national defense, considering whether protection from terrorism should be a governmental or industrial obligation, as well as the societal costs of adopting a policy of "zero" risk from terrorist actions.

Mr. Gaukler is a partner with Shaw Pittman LLP in Washington, D.C. Mr. Barnett and Mr. Rosinski are associates at Shaw Pittman. They may be reached at paul.gaukler@shawpittman.com, sean.barnett@shawpittman.com, and douglas.rosinski@shawpittman.com, respectively.

Since September 11, people have worried that nuclear power plants are vulnerable to an array of postulated terrorist acts, such as deliberate crashes of airliners like those occurring on September 11, use of truck bombs like the one used to destroy the federal building in Oklahoma City, sabotage by plant "insiders," military-style assaults by groups of armed individuals, attacks using biological and chemical agents, and cyber attacks. The challenge for policymakers and the industry is to evaluate whether our heightened awareness since September 11 of these or other potential terrorist threats requires additional security measures beyond those presently in place at nuclear plants, and if so, how these threats should be addressed. NRC's current comprehensive reevaluation of its security requirements in light of September 11 is prudent, not just for nuclear plants, but for our national infrastructure generally. However, we counsel against adopting potentially burdensome security measures without consideration of whether they are truly necessary, for the institution of such measures could deny our society the benefits of nuclear plants or other critical infrastructure.

Nuclear power originated as a government monopoly and, ever since the Atomic Energy Act of 1954 authorized its commercial use by private industry, commercial nuclear power has been subject to strict federal regulation and oversight. As a result, U.S. commercial nuclear plants are the most closely regulated of our nation's infrastructure and probably the strongest, most secure industrial facilities ever constructed. Nuclear plant security is designed to be far superior to that provided at other critical infrastructure facilities—such as dams, chemical plants, and liquid natural gas facilities—whose destruction would pose equal, if not greater, public risk. Much of the strength of nuclear plants results from the nature of the facilities themselves. The operating temperatures and pressures of the equipment, piping, and devices used to generate electricity at nuclear plants require structures and components of enormous strength and resiliency. Further, nuclear plants must meet rigorous NRC design criteria and quality assurance requirements intended to protect public health and safety from the uncontrolled release of radioactivity. 10 C.F.R. Part 50, App. A and B. These design criteria address the containment of radioactive material, the cooling of the reactor, and the prevention of nuclear chain reactions. They also require extensive fire protection measures and the ability to withstand hurricanes, tornadoes, and earthquakes. Key systems

must be designed so that the failure of any single component would not prevent the system from functioning (e.g., providing cooling water to the reactor core). Important systems must be completely redundant and independent of each other.

These design and quality requirements yield structures capable of withstanding events that would destroy or significantly damage ordinary facilities. The strength of nuclear plants is exemplified by the thick, heavily reinforced concrete containment structure that houses the reactor. Typical reactor containments have walls 3½ feet to 6 feet thick.

Thus, although not specifically designed to resist the crash of a hijacked aircraft, the containment structure would provide extensive protection from such a crash. The containment's thickness, heavy reinforcement, and shape enables it to resist extreme external pressures, even pressures similar to those that might be produced by the impact of a modern jet airliner. Thus, even if a pilot could successfully hit the containment (a relatively small target compared to either the Pentagon or the World Trade Center), the containment would most likely resist the force of such an impact. When Sandia National Laboratories in a 1988 test crashed an F-4 fighter aircraft directly into a simulated containment wall at a speed of 481 mph, the aircraft shattered into pieces and only penetrated about two inches into the reinforced concrete wall. W.A. von Riesemann et al., *Full-Scale Aircraft Impact Test for Evaluation of Impact Forces*, TRANSACTIONS OF THE 10TH INTERNATIONAL CONFERENCE ON STRUCTURAL MECHANICS IN REACTOR TECHNOLOGY, AUGUST 14–18, 1989, ANAHEIM, CALIFORNIA, USA, J-285 (1989). The slight damage caused by this simulated accident strongly suggests that the containment would prevent aircraft components from penetrating into the building's interior, contrary to what occurred at the World Trade Center, and thus would also most likely prevent any jet fuel from reaching the building's interior. Even a large jet fuel fire outside the reactor containment building would burn relatively quickly (as the fuel would be distributed over a large area by the force of the aircraft impact) and would not threaten the reinforced concrete containment structure housing the reactor. If the aircraft crashed into other parts of the facility, redundant, independent, and physically separate safety systems would protect the nuclear fuel and allow the plant to shut down safely.

Moreover, NRC regulations also address risks from truck bombs like the one used in Oklahoma City in 1995. Specifically, 10 C.F.R. § 73.55(c)(8) requires that barriers be erected to preclude vehicles from reaching a point where an explosion could damage the reactor or critical plant systems.

Another worry expressed is that nuclear plant spent fuel pools might be vulnerable to terrorist attacks. After its use in the reactor, nuclear fuel (in the form of assemblies of long, thin, hollow rods of zirconium containing fissionable uranium dioxide) is transferred to the spent fuel pool for cooling and storage pending its permanent disposal or removal to an alternative storage location. Concerns over the spent fuel pool typically assume that the pool is completely or mostly drained of its water and that the zirconium metal surrounding the spent fuel ignites, releasing a plume of radioactive material. However, it would be difficult to drain a spent fuel pool of its water in a short time. Designed to withstand earthquakes and tornadoes, the walls of the pools are reinforced concrete, typically 4 feet to 5 feet thick, lined with stainless steel, and at many plants are partly sunk into the ground. Most pools are somewhat smaller in area than an Olympic swimming pool and typically are 55 feet to 60 feet deep. The pools are designed so that water cannot be drained or pumped using plant systems below a level well above the spent fuel rods (approximately 10 feet to 20 feet). *See* NRC, TECHNICAL STUDY OF SPENT FUEL POOL ACCIDENT RISK AT DECOMMISSIONING NUCLEAR POWER PLANTS (Oct. 2000) (NRC Report) at 3-5, 3-18, A1A-2. Purposely draining the pool to uncover the rods would require removing thousands of gallons of water using makeshift pumping arrangements and would take many hours, if not days, of pumping to accomplish. *See* NRC Report at A2A-38. Further, using generally accepted calculations, we estimate that a large amount of explosives would be required just to crack the thick reinforced concrete pool walls and stainless steel liner, let alone blast a hole large enough to drain the pool. Because NRC regulations require barriers to prevent potential truck bombs from reaching vital plant areas, such as the spent fuel pool, it would be difficult to drain the pool using explosives.

Since the Atomic Energy Act of 1954 commercial nuclear power has been subject to strict federal regulation and oversight.

Even if the pool were successfully drained, it would be remarkably difficult to ignite the fuel rods. Very specific conditions—a tremendous amount of heat with little or no heat removal—are required to initiate a "fire" of the zirconium fuel cladding. A nearby explosion or fire would not be enough. NRC has conservatively estimated that, even if a pool were drained to uncover the

fuel and no cooling was available, it would take hours (up to more than a day depending on the age of the spent fuel) for the heat produced by the radioactive decay of the spent fuel to raise the fuel cladding temperature to 900º C, the postulated ignition temperature of zirconium. NRC Report at 2-3. Even then, it is unclear whether ignition would occur, for a zirconium nuclear fuel rod has never actually been ignited at 900º C. *See generally* NRC Report, App. 1.B.

Although concern has been expressed that an aircraft crash might cause the spent fuel rods to ignite, it is highly improbable that a crashing hijacked aircraft could create the necessary conditions for this to occur. The thick reinforced concrete wall around the pool, the building covering the pool and shielding it from view, the 10 feet to 20 feet or more of water above the spent fuel, and the small surface area of the pool make it unlikely that a pilot could crash an aircraft in the precise location and manner required to damage and drain the pool in order to potentially cause a zirconium fire. The fire from 20,000 gallons or more of jet fuel would not cause a zirconium fire in an intact pool because of the depth of the water above the spent fuel rods. Nor, as can be shown by simple calculations, would the fire produce enough heat to boil away much of the water. Finally, nuclear plant staff are extensively trained and well equipped to fight plant fires, *see* 10 C.F.R. Part 50, App. R., and would be expected to respond promptly and mitigate both the effects of the crash and its potential for causing a zirconium fire, such as replenishing the spent pool water inventory from readily available alternative sources, such as the fire pump.

Similar concerns have been raised regarding the vulnerability of nuclear plants undergoing decommissioning as well as dry cask storage facilities at which spent nuclear fuel may be stored. NRC's comprehensive review of its security requirements in light of September 11 will cover both. There are roughly a dozen plants currently undergoing decommissioning. At those plants, the nuclear fuel is completely removed from the reactor, but it could remain in the spent fuel pool pending its permanent disposal (or, alternatively, it could be removed from the pool and stored in dry storage casks). If the fuel remained in the pool, its vulnerability to terrorism would be low, just as in an operating plant. Although a decommissioning plant would likely possess fewer redundant systems and staff for firefighting or security than an operating plant, the fuel at a decommissioning plant would be older and cooler, and hence would have less potential for igniting a zirconium fire. For example, NRC has concluded that unobstructed natural air convection cooling by itself, absent any water in the pool, would be sufficient to preclude a zirconium fire for spent fuel removed from a reactor for five years. NRC Report at A1A-4. Dry storage casks in which spent fuel could also be stored would also provide substantial protection against terrorism. Such storage casks typically have concrete and steel walls 2 feet to 3 feet thick, *see, e.g.,* Final Safety Analysis Report for the HI-STORM 100 Cask System, NRC Docket No. 72-1014 § 1.2.1 (2000), which would provide significant protection against penetration by a crashing aircraft or other forms of attack. *See, e.g.,* P.R. Davis, D.L. Strenge, and J. Mishima, Accident Analysis for Continued Storage (Oct. 27, 1998). The reinforced concrete walls would also protect the spent fuel from even large jet fuel fires; it would take hours for the heat from an external fire to be conducted through a cask wall and begin to effect the spent fuel inside the cask. *See, e.g.,* HI-STORM 100 FSAR at 11.1-16, 11.2-13.

In addition to potential attacks involving direct physical impacts, recent House of Representatives legislation, H.R. 2983, also would require evaluation of nuclear plant vulnerability to biological and chemical attacks. While such an evaluation may be useful, provisions are already in place to mitigate chemical and biological attacks against nuclear reactors. NRC design criteria require plant control rooms to remain habitable even under adverse environmental conditions so that operators can shut down the reactor. *See, e.g.*, 10 C.F.R. Part 50 App. A, Criterion 19. Accordingly, control rooms are sealed and air intakes are filtered to minimize the rate at which toxic gases (or biological agents) could enter. Control rooms are also equipped with self-contained breathing apparatus. Thus, control room operators should be able to safely shut down the plant following a biological or chemical attack. Further, NRC regulations require reactors to have the capability of being shut down from a location outside the control room, *see, e.g.,* 10 C.F.R. Part 50 App. R, so an attack that might disable the control room would not defeat the capability of shutting a plant down safely.

H.R. 2983 also would require evaluation of nuclear plant vulnerability to biological and chemical attacks.

H.R. 2983 would also require evaluation of nuclear plant vulnerability to cyber attacks. Presumably, such attacks would involve attempts to remotely seize and manipulate plant controls to cause an accident. Critical functions at nuclear plants, however, are not vulnerable to cyber attacks. Computers are used only to monitor plant performance and system readiness for administra-

tive purposes, not to provide input for control of plant equipment. Only NRC-licensed personnel operate plant controls, *see* 10 C.F.R. Part 55, and they operate and monitor the plant using instrumentation and alarms directly wired to plant sensors and equipment. They neither monitor plant functions nor operate plant equipment using computer controls.

Commercial nuclear plants are also required by NRC regulation to institute stringent physical security provisions. 10 C.F.R. § 73.55. A security organization and plant physical protection systems must be in place to prevent unauthorized access of personnel, vehicles, and materials; ensure only authorized activities are conducted; permit only authorized handling of nuclear material; and detect and respond to unauthorized penetrations. The entire plant perimeter must be fenced with adjacent areas cleared to permit observation of both sides of the fenced barrier. The perimeter must be monitored both visually and electronically with electronic alarms sounding at two independent, continuously staffed stations. Entry points must be guarded and monitored and access must be strictly controlled. All plants must have armed response forces whose qualifications and tactical training are dictated by 10 C.F.R. Part 73, App. B. Each armed responder or watchman must be capable of maintaining continuous communication with each of the continuously staffed alarm stations.

These measures must be designed to protect against attacks from external armed groups and saboteurs inside the plant. All nuclear plants are required to defend against a "design basis threat," defined in 10 C.F.R. § 73.1(a)(1) as "[a] determined violent external assault, attack by stealth, or deceptive actions, of several persons" assumed to have military training, automatic weapons and explosives, a vehicle for transportation, and assistance by an insider within the plant. A formal Safeguards Contingency Plan must be developed and maintained in accordance with 10 C.F.R. Part 73, App. C, identifying a predetermined set of threat–response actions, their means of implementation, and those responsible for responding to threats. Further, nuclear plants are required to establish and document a working liaison with local law enforcement authorities that they can summon for assistance in the event of an attack.

Under these contingency plans, threats at nuclear plants would be countered by an armed tactical force permanently stationed at the plant, whose mission is to quickly determine a threat's existence, assess its magnitude, and interpose itself between the threat and specific key plant areas. The capability of security response forces and systems to defend against threats must be regularly tested in live exercises monitored by NRC using mock attack forces. *See* NRC INSPECTION MANUAL, Inspection Procedure 81110, Operational Safeguards Response Evaluation (OSRE) (July 1, 1997). If weaknesses are identified, the plant must institute additional defensive countermeasures, such as explosive-resistant barriers or hardened bunkers. *Id.*

Media reports have claimed that nuclear plants have "failed" in nearly half of the OSRE force-on-force exercises evaluated by NRC. However, OSRE exercises are specifically designed by knowledgeable NRC security specialists to test potential vulnerabilities identified in a plant's security systems to determine whether improvements are needed. Accordingly, weaknesses found during an OSRE evaluation do not represent "failures" in which a real attacking force would necessarily have succeeded in causing serious damage to the plant. *See* Letter from NRC Chairman Richard Meserve to Senator James Jeffords (Dec. 17, 2001) (Jeffords Letter).

OSRE exercises are designed by NRC to test potential vulnerabilities in a plant's security systems.

To provide additional protection against sabotage by insiders, access to nuclear plants must be restricted to rigorously screened and authorized personnel. The screening process requires (1) a background investigation, (2) a psychological assessment, (3) drug and alcohol screening, and (4) continuous behavioral observation. 10 C.F.R. §§ 73.56(b)(2); 10 C.F.R. Part 26. Each person entering the plant must be searched for weapons, security personnel must visually confirm the identity of authorized personnel entering the plant, and all packages must be screened. Visitors must be accompanied at all times by authorized personnel. 10 C.F.R. § 73.55(d). Inside the facility, personnel must be monitored by security cameras or other electronic means. Access to sensitive plant areas must be controlled by electronically keyed or coded security doors that are monitored and alarmed for improper or unauthorized access. Security computers must continuously monitor key locations within the facility and can disable security doors if necessary. *See* 10 C.F.R. §§ 73.55(d) and (e).

Another layer of protection to the public is provided by the plants' emergency response plans. Nuclear plants are required to have plans, dedicated facilities, and equipment in place to mitigate the consequences of an emergency. 10 C.F.R. § 50.47. Emergency plans must provide for assessment, radiation monitoring,

prompt notification of governmental officials, fire and damage control, public communication, coordinated evacuations, and medical services. Nuclear reactor emergency plans are unique in requiring planning for the evacuation of the surrounding population out to approximately 10 miles from the plant. 10 C.F.R. Part 50 App. E § IV.G; 10 C.F.R. § 50.47(c)(2). These plans must be approved by both the NRC and the Federal Emergency Management Agency, *see* 10 C.F.R. § 50.47(a)(2), and must be tested in biennial exercises in which state and local authorities participate.

All of these security requirements are subject to NRC's broad enforcement authority under the Atomic Energy Act, which is primarily implemented through stringent self-reporting requirements, *see, e.g.*, 10 C.F.R. §§ 50.72, 50.73, extensive routine and special inspections, and full-time resident inspectors at each nuclear power plant. 10 C.F.R. § 50.70. Nuclear plants must document and track deviations from regulations or plant design, whether identified by the operator, NRC staff, or a third party. 10 C.F.R. Part 50, App. B, Criterion XVI. Violations of NRC regulations are subject to sanctions, including steep fines and license suspension or revocation; deliberate misconduct is subject to criminal prosecution. 10 C.F.R. Part 2, Subpart B.

In sum, nuclear plants already have extensive measures in place to prevent, withstand and, if necessary, mitigate the effects of a terrorist attack. Thus, they are unlikely to be attractive targets for sophisticated terrorists, reluctant to launch attacks that would likely fail. Additional precautions that might reasonably further reduce the risk from terrorism should of course be considered and both NRC and the industry are prudently reviewing nuclear plant security in light of September 11. Heightened security measures at nuclear plants mandated by NRC since September 11 include augmented security forces and patrols, increased coordination with law enforcement and military authorities, additional site access limitations for personnel and vehicles, as well as other short-term and longer-term actions to strengthen plant capability to respond to terrorist attacks. *See* Jeffords Letter. Further, NRC has explicitly advised Congress that it will be reviewing and updating its design-basis threat in light of September 11. *Id.* Moreover, as evidenced by recent legislative proposals and NRC responses to congressional inquiries (such as the Jeffords Letter), Congress and the executive branch are closely monitoring NRC's response to the events of September 11. Judging by previous health and safety evaluations undertaken by NRC, the federal government, and the nuclear industry (such as those which occurred in the wake of the Three Mile Island accident in 1979), it is safe to predict that a comprehensive review will be performed and appropriate enhancements will be implemented.

Nuclear plants already have extensive measures in place to prevent, withstand, and mitigate the effects of a terrorist attack.

Comparison to Security of Other Infrastructure and Hazardous Activities

Compliance with NRC regulations makes commercial nuclear plants significantly less vulnerable to terrorism than other infrastructure facilities. Our industrial infrastructure as a whole is simply not designed to withstand terrorist attacks. For example, one of the most worrisome potential targets identified in Washington, D.C. following September 11 was not the Capitol or the White House, but a water treatment facility located roughly a mile away. Reportedly, 40,000 tons of deadly chlorine gas was stored there, unprotected and unguarded in 90-ton rail cars. The rupture of just one rail car reportedly could have placed 1.7 million people at risk. This highly toxic chemical was quickly removed and replaced with a less dangerous substitute.

These dangers are not isolated. As reported in the December 16, 2001 *Washington Post*, the Environmental Protection Agency (EPA) has determined that "[a]t least 123 plants each keep amounts of toxic chemicals that, if released, could form deadly vapor clouds that would put more than 1 million people in danger" and "[m]ore than 700 plants could put at least 100,000 people at risk." Yet there are no "nuclear style" containment structures or federal security requirements for chemical plants and refineries. EPA counts on the facilities undertaking necessary precautions "voluntarily."

Another terrorism scenario posing comparable public risk is a fuel-air explosion, caused by the vaporization and ignition of volatile fuels or gases, which reportedly has the explosive power of many tons of TNT. A suicide bombing, for example, could transform a liquid natural gas (LNG) tanker or storage tank into a weapon of mass destruction. Indeed, Representative Edward Markey (D-MA) claimed in an October 1979 letter to the *Boston Herald American* that an LNG accident "might lead to a catastrophe on a par with the worst nuclear power plant accident, producing a fire storm destroying everything in its path."

Despite their potential risks, these facilities are not designed to withstand the types of threats from which nuclear plants are protected. NRC regulations are virtu-

ally unique in requiring analyses of highly improbable events that, if analogously applied to these facilities, would prohibit the use of thin storage tanks, railcars, or warehouses to hold industrial quantities of toxic, flammable, and explosive materials. Such comparison demonstrates the relative security of nuclear plants from terrorism vis-à-vis other critical infrastructure and that society could benefit more from strengthening the security of these other, less secure, critical infrastructure facilities.

NRC security regulations are potentially transferable to other industrial settings. For example, an October 19, 2001, *Baltimore Sun* article described poor security at the nation's seaports. The article cited a 1999 presidential panel finding that many of the nation's largest seaports suffered from physical security shortcomings or failed to perform criminal background checks on employees. Some seaports may lack even ordinary precautions such as gates, fencing, and cameras. For instance, port warehouses described in the article contained unguarded stockpiles of numerous toxic chemicals within a mile of a densely populated downtown metropolitan area. NRC security requirements regarding fencing, vehicle barriers, intrusion detection systems, armed guards, and formal liaison agreements with local law enforcement would appear to provide a good model for seaports and other critical infrastructure, such as chemical plants and LNG facilities. Further, according to a November 2001 report by Bracewell & Patterson, DOE's Office of Critical Infrastructure, which has primary federal responsibility to protect energy infrastructure terrorism, lacks regulations to compel facilities to participate in its security program. NRC regulations could serve as a model for DOE regulations that could address terrorism security risks.

The nuclear industry is a leader in emergency response planning.

The NRC model could also help reduce non-nuclear facility vulnerability to internal sabotage. The quality of the NRC screening process used to qualify people for facility access helps place nuclear plants among those civilian facilities best protected against sabotage. NRC access regulations and the nuclear industry's extensive experience in effectively implementing background investigations, psychological testing, and personnel reliability programs provide a useful model for screening employees of airports (where employee screening processes have been roundly criticized since September 11), seaports, chemical facilities, and other sensitive infrastructure.

The nuclear industry is also a leader in emergency response planning, particularly with respect to response actions and potential evacuations of surrounding communities. It has developed considerable expertise in coordinating industry, federal, state, and local organizations to respond to potentially large, complex emergencies. The nuclear plant approach could serve as a useful model for agencies charged with integrating security and emergency response organizations, such as the new Office of Homeland Defense.

Policy Issues Presented by the Events of September 11

The concerns expressed by Congress and others regarding nuclear plant security since September 11 raise important national policy issues. The first issue is whether placing special emphasis on nuclear power plant security is a proper allocation of government and private industry resources. As noted, there are numerous other infrastructure facilities that are as potentially hazardous as nuclear plants, yet lack the defense of the in-depth mechanisms in place at nuclear plants. Comparatively more societal benefits would be gained by enhancing security at those other facilities. Indeed, NRC security regulations could be used as a model for such an effort. In a world of limited resources, strengthening the overall security of our nation's infrastructure would yield far greater benefits than would using the same limited resources to upgrade the existing security at nuclear power plants.

A second policy issue important in protecting national infrastructure generally is the division of responsibility between private industry and national defense and security. Should individual facilities be required to defend themselves against all threats or should the defense against some threats (e.g., those from foreign enemies such as Al Qaeda) be the responsibility of the military, FBI, intelligence agencies, or state and local law enforcement?

The issue of foreign enemies potentially attacking U.S. infrastructure facilities was raised thirty-five years ago in a hearing before the Atomic Energy Commission (the predecessor to NRC) in connection with nuclear power plant licensing. As enunciated there, the Commission's policy has been that "protection . . . against hostile enemy acts is a responsibility of the nation's defense establishment" and internal security agencies, and not of the Commission or individual facilities. *Florida Power & Light Co.* (Turkey Point Nuclear Generating Units 3 and 4), 4 AEC 9, 13 (1967), *aff'd, Siegel v. AEC,* 400 F.2d 778 (D.C. Cir. 1968). The Commission's rationale for that position is grounded in practical reality:

> One factor underlying [the Commission's] practice in this connection has been a recognition that [facility] design features to protect against the full range of the modern arsenal of weapons are simply not practicable and that the defense and internal security capabilities of this country constitute, of necessity, the basic "safeguards" as respects possible hostile acts by an enemy of the United States.
>
> The circumstances which compel [the Commission's] recognition are not, of course, unique as regards a nuclear facility; they apply also to other structures which play vital roles within our complex industrial economy. The risk of enemy attack or sabotage against such structures, like the risk of all other hostile acts which might be directed against this country, is a risk that is shared by the nation as a whole. This principle, we believe, is rooted in our political history and we find no Congressional indication that nuclear facilities are to be treated differently in the subject regard.

Turkey Point, 4 AEC at 13.

The latter point—that risk of enemy attack against critical facilities such as nuclear plants is shared by the nation as a whole—is the most compelling reason for keeping the responsibility for defending against terrorism with the nation's defense and internal security apparatus. Nuclear plants are clearly not the only potential targets in the United States. Attacks against chemical and natural gas facilities, seaports, refineries, hydroelectric dams, and sports stadiums, among others, could result in large numbers of casualties. Moreover, terrorist groups operating within the United States could directly target civilians or assassinate political leaders, as they have elsewhere. Beyond the loss of human life, destruction of critical infrastructure, such as pipelines, refineries, transmission lines and the like, could also have serious economic impacts.

The multitude of potentially vulnerable targets in the United States dictates that we focus on stopping foreign terrorist attacks at their inception rather than repulsing them at their targets. Only the government can take steps, such as the war in Afghanistan, to forestall the terrorist threat before it reaches our shores or to implement the necessary security measures at our airports, borders, and coastlines. Further, only the government has the intelligence and law enforcement capability to track potential terrorists and to prevent their launching attacks in the first place. Thus, it is reasonable that responsibility for forestalling terrorist threats should rest with the government, and the cost of defending against terrorism be borne by the nation as a whole.

Additionally, the cost of hardening and defending every vulnerable target against potential attack (whether funded privately or by the government) would be much higher than the cost of protecting the nation as a whole. A strategy of defense at the target would require all of our potentially vulnerable facilities —as well as concentrations of people and our political leaders—to be defended as military fortresses. As the Commission recognized decades ago, such an approach is impracticable and socially undesirable. An active, global approach, in which centralized assets—intelligence, law enforcement, or military—respond to threats here or abroad, is much more efficient than one in which security assets are deployed at each facility to respond just to attacks on that facility. Moreover, this "global" approach need not be implemented entirely at the national level. Security assets at the state or local level (e.g., the National Guard and law enforcement organizations) could be responsible for appropriate regional actions, such as providing specially trained forces for immediate response to terrorist threats. Coordination and sharing information at the national level would ensure global coverage, but local implementation would allow the tailoring of assets and response plans to local situations.

Thus, nuclear plants and other critical infrastructure should be required only to defend against threats that are deemed likely to evade interception by authorities. NRC regulations described above, which the NRC is reviewing in light of September 11, already provide for such protection at nuclear plants by requiring physical protection measures and armed security forces.

The third policy issue arising from recent concerns expressed about nuclear plant security is how much protection we as a society should seek in light of September 11. Some argue that no level of protection against terrorism—and hence no burden on nuclear plants—is too high. However, nuclear energy is an integral part of the nation's infrastructure and currently provides more than 20 percent of our nation's electricity. Nuclear energy does not create air pollution and also provides a means of reducing U.S. greenhouse gas emissions. Unnecessarily increasing the cost of protecting nuclear plants—or shutting them down altogether—would deny these benefits to society.

More generally, arguments that no level of protection is too much ignore the continual tradeoffs that our society makes between risks and benefits. We drive cars and fly airplanes despite the potential for accidents. We build chemical plants, oil refineries, and hydroelectric dams to reap their benefits while accepting some risk relating to their operations. We seek to minimize risk, but we do not insist on zero risk. Doing so would deny society the benefits provided by these activities and technologies. Consistent with this principle, the NRC has established as one of its overarching safety goals that the "[s]ocietal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks." 51 Fed. Reg. 30,028, 30,029 (1986).

This same logic applies equally after September 11 as before. If we demanded absolutely no risk from terrorism, no planes would fly, bridges would be closed, and buildings would be emptied even though we as a society are otherwise exposed to risk daily. For example,

the yearly risk from dying in a car accident is one in seven thousand. Thus, if we are to continue to exist as a modern, technological society, we cannot insist on "zero" risk from terrorism, or from any other cause.

We should continue to assess the risk from terrorism directed at nuclear plants and seek to minimize it through reasonable security provisions. But we should also be mindful that its benefits, as any other socially beneficial activity, could be diminished or negated by excessive security burdens. The burdens on nuclear plants to protect against terrorist attacks should be reasonable in light of the benefits of nuclear power and the risk of radioactivity release and comparable to the equivalent benefits and risks associated with other critical infrastructure facilities.

Nuclear power plants are among the least vulnerable and most resilient of our nation's infrastructure to terrorist attacks. Our open, modern technological society, with myriad infrastructure facilities, cannot blindly comply with calls for "zero" risk as sought by some. Further, policymakers need to recognize that there is a point at which industrial security must become national defense. This does not mean we should not review the safety and security of nuclear plants in light of September 11. All industrial and infrastructure facilities should undertake such a review, as the NRC is currently doing for nuclear plants, and implement improvements reasonable and consistent with the actual threat to public health and safety. On the basis of our assessment, however, we do not believe that the extreme actions called for by some, such as the shutdown of all nuclear plants or the deployment of large guard forces armed with anti-aircraft missiles, are warranted. Rather, security against terrorism should be based on the actual terrorism threat and the benefits and costs to society of providing additional protection against it.