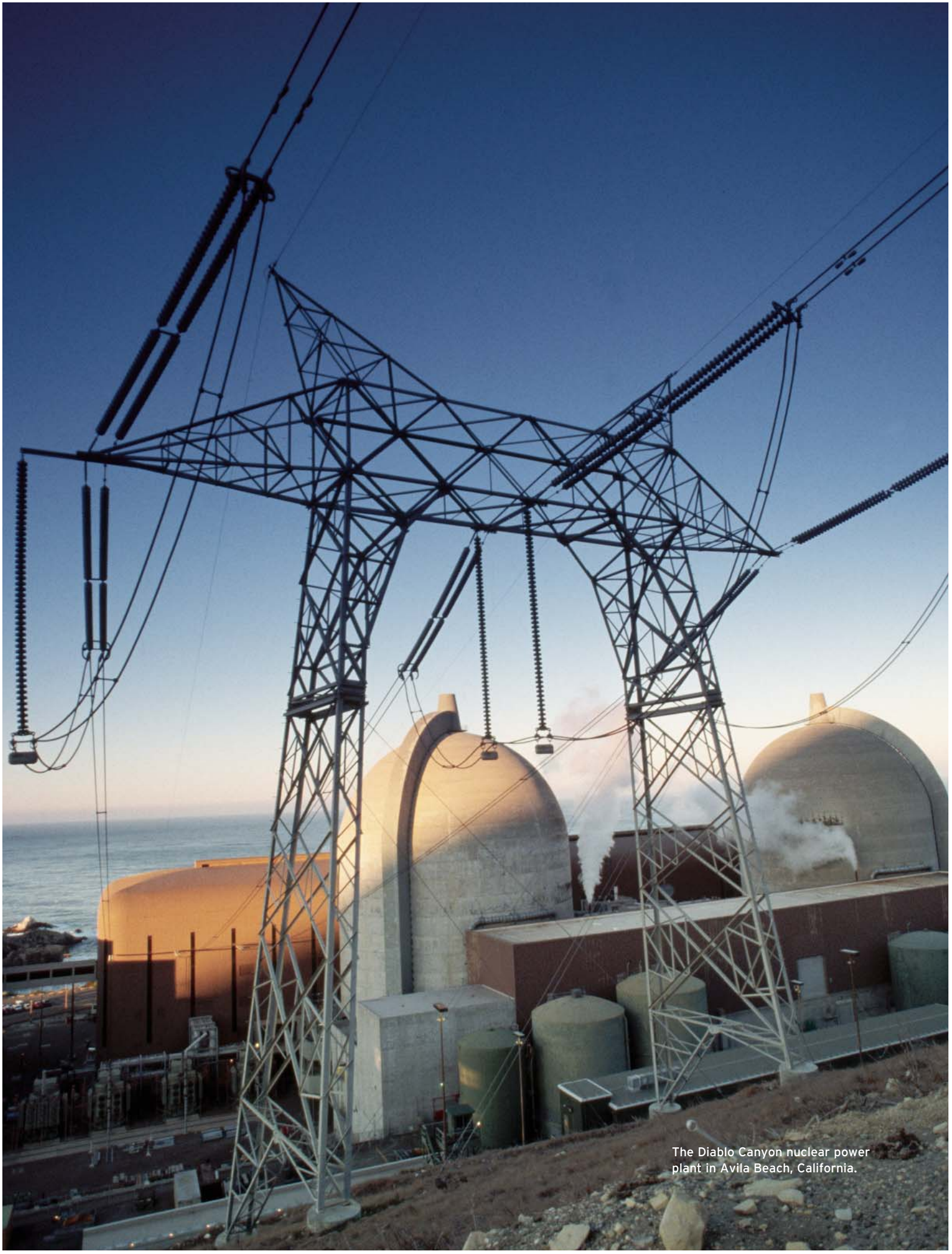


The Diablo Canyon nuclear power plant in Avila Beach, California.

THE NRC'S DIRTY LITTLE SECRET

By Daniel Hirsch,
David Lochbaum & Edwin Lyman

The Nuclear Regulatory Commission is still unwilling to respond to serious security problems.

FOR A QUARTER OF A CENTURY, THE NUCLEAR Regulatory Commission (NRC) kept its dirty little secret: Despite the fact that a successful attack on a U.S. nuclear plant could cause thousands of illnesses and deaths in the surrounding area, and despite the clear increase in terrorist threats over that same period, the commission continued to require the country's nuclear power plant operators to maintain only a minimal security capability.

The NRC has not required nuclear facilities to guard against an assault by more than three attackers—and never with the help of more than a single insider. In addition, for purposes of planning security, the NRC assumed that the three attackers would act as a single team, armed with nothing more sophisticated than hand-held automatic rifles.

More troubling, the commission has not required plant operators to be able to withstand a possible attack by boat or plane—nor to have the capacity to defend in any way against an attack by anyone defined as "enemies of the United States"—nations or sub-national groups.

After September 11, 2001, when 19 Al Qaeda recruits acting in four coordinated teams used commercial airliners to attack the World Trade Center and the Pentagon, a great deal of concern was expressed about U.S. nuclear plants' vulnerability to terrorist attack, and questions were raised about increasing security at nuclear facilities. In early 2002, it was widely believed that the NRC would finally upgrade its 25-year-old "design basis threat"—the maximum threat that nuclear plant security systems are required to protect against—and that considerably higher standards would be established.

A non-response

Although the commission has never advertised the limitations of its design basis threat (DBT), the guidelines are no secret to terrorists. The NRC has long published its security requirements in the Code of Federal Regulations, available at any library or on the Internet, and sup-

Daniel Hirsch is president of the Committee to Bridge the Gap. David Lochbaum is a nuclear safety engineer with the Union of Concerned Scientists. Edwin Lyman is president of the Nuclear Control Institute.

ROGER RESSMEYER/CORBIS

plemental information can be found in other publicly available NRC documents.[1] And critics have been pointing out the inadequacy of those security requirements for decades.[2]

Although the nuclear power plants' required security arrangements are minimal, even a modest attacking force—one that fits the NRC's definition—can easily overwhelm the security guards at many U.S. nuclear plants, as demonstrated by the NRC's own force-on-force testing program, known as the Operational Safeguards Response Evaluation (OSRE). At nearly half the nuclear plants where security has been OSRE-tested, mock attackers have been able to enter quickly and simulate the destruction of enough safety equipment to cause a meltdown—even though the reactor operators typically have been given six months' advance notice of the day of the test.

In response to these dismal test results, the NRC attempted to quietly kill off the test program.[3]

Since the massive terrorist attacks of September 11, the NRC's inaction has been even more troubling. Despite the obvious attractiveness of U.S. reactors as terrorist targets, the NRC and the nuclear industry have done little to upgrade security.

As this article went to press in mid-April, the regulations remained unchanged. The NRC is considering some sort of modest upgrade that could be issued soon, but it appears to postulate a far smaller assault than that which occurred on September 11. Meanwhile, the NRC and the nuclear industry strenuously lobbied Congress to prevent it from passing legislation that would have forced the NRC to raise the DBT to match the level of attack on September 11.

Additionally, the OSRE defensive tests were discontinued after September 11, and are only now being revived with a few "volunteer" plants whose owners presumably are confident they can pass.

On January 17, 2002, then–NRC Chairman Richard Meserve gave a speech at the National Press Club, titled "Nuclear Security in the Post–September 11 Environment," arguing that little was needed to improve what he characterized as "very strong" reactor security. "First, and most important," he said, "since September 11 there have been no specific credible threats of a terrorist attack on nuclear power plants." Just 12 days later, however, President George W. Bush said in his State of the Union address that diagrams of American nuclear power plants had been found in Al Qaeda camps in Afghanistan.

One must ask why the NRC is so reluctant to require greater security efforts. There are two obvious answers: Improving security at reactors will cost money; and it may remind the public of the risks associated with nuclear power, making expansion of the nuclear sector, as proposed by the industry and urged by the Cheney energy task force, more difficult. But should political factors be permitted to interfere with protecting the population?

The endless review

In March 2002 NRC Commissioner Jeffrey Merrifield defended the commission's apparent lack of progress by quoting Hemingway's admonition

Beamhenge?

A successful terrorist attack on a U.S. nuclear power plant would pose a higher risk and come at a greater cost than an assault on nearly any other target. Dozens of U.S. nuclear plant sites have the potential of exposing hundreds of thousands of people to radiation that would be dispersed in the air; that radioactivity would also render large and valuable areas of land essentially uninhabitable for many decades.

Yet efforts to harden these nuclear targets have not even begun, even though the need to protect them became painfully clear on September 11, 2001, when the vulnerability of major structures to attack by aircraft was stunningly demonstrated. Instead, the Nuclear Regulatory Commission and its constituency of cost-sensitive energy companies has stumbled along, at first denying the problem, then offering political excuses as to why it cannot take decisive action to protect the public.

The nuclear industry asserts that the cost and time it would take to significantly harden or retrofit these power plants makes taking safety measures impractical. But what if there were a low-cost way to quickly improve a nuclear facility's survivability?

There is a way. It's called "Beamhenge."

Beamhenge is simply a line of steel beams set vertically in deep concrete foundations connected by bracing beams, a web of high-strength cables, wires, and netting linking the vertical beams to form a protective screen—the nuclear-grade equivalent of the fences erected around golf driving ranges. Beamhenge would not need to completely encircle the nuclear plant—it would merely need to shield the vulnerable side or sides of the facility's key structures. Depending on the nuclear plant's geography and vulnerabilities, Beamhenge could be a single row of closely spaced beams or multiple

to "never mistake motion for action." It seems instead as if the NRC is hoping that the public will mistake paralysis for action.

Soon after September 11, the NRC announced that it was undertaking a "top-to-bottom" review of its security programs. But the review had no timelines or specific goals. Instead, it has become a graveyard for fundamental policy issues the commission is loathe to address. In the meantime, U.S. nuclear power plants remain dangerously vulnerable to terrorist attack.

The NRC continues to "study" three issues concerning potential damage—the effects of large commercial aircraft attacks on nuclear plants; the impacts of attacks with explosives on spent fuel pools; and the health and environmental consequences of terrorist attacks on nuclear plants.

Another set of issues concerns the nature of defense—the appropriate design basis threat after September 11; the appropriate role of civilian law enforcement and the military in protecting privately owned nuclear plants; and the appropriate qualifications, training, and work schedule of plant security guards.

March 18: Connecticut Gov. John Rowland (center) arrives at the Millstone nuclear power plant in Waterford to review its security preparations.

Even if the review is completed, most results are unlikely to see the light of day because the commission will deem them too sensitive to release. Yet when members of the public, the media, and elected officials demand to know what the NRC has done to increase security, it says little and simply points to the ongoing review.

In the meantime, after more than five months of resisting the call to require security upgrades at nuclear power plants, in February 2002 the commission finally issued a set of mandatory "interim compensatory measures," or ICMs. Although the details of these measures are secret, the NRC has characterized them as providing "additional protection against vehicle bombs, as well as water- and land-based assaults . . . requirements for increased security patrols, augmented security forces,

rows of more widely spaced beams. The height of the beams and the length of the Beamhenge would depend on the configuration being protected from likely incoming trajectories.

The main purpose of Beamhenge would be to slow down an attack, fragment the attacking aircraft into smaller pieces, disperse the mass of jet fuel, and protect the more vulnerable containment, spent fuel pool, and other structures located within the perimeter from being breached by the mass of the projectiles. The beams would tend to scatter the jet fuel and slow down other projectiles like the fuselage.

The structure would also provide some degree of protection against surface-to-surface and air-to-surface missiles, as well as other ballistic and self-propelled ordnance. The metal mesh netting strung between the vertical beams would not stop a projectile, but would serve to trigger detonation of its warhead before it reached the facility's walls.

In fact, the possibility that an attack by air would lead to a catastrophe could be rendered from "more likely than not" to "essentially unlikely" for the expenditure of a fraction of one percent of the construction cost of the average facility, and the protective structure could be built in a few months. Even if the project were evaluated in terms of economic costs only, with no consideration of the value of human lives, a price in the low tens of millions of dollars for each facility should be difficult to resist. The total cost may seem high, but it would still be less than the total of the one-time loans the government arranged for the airline industry in the days following September 11.

A more pertinent question—one the public should be asking now, before terrorists strike again—is why the Nuclear Regulatory Commission has yet to implement a project like Beamhenge.

Joel Hirsch

Joel Hirsch, an attorney, represents the Committee to Bridge the Gap in Los Angeles, California.

ASSOCIATED PRESS

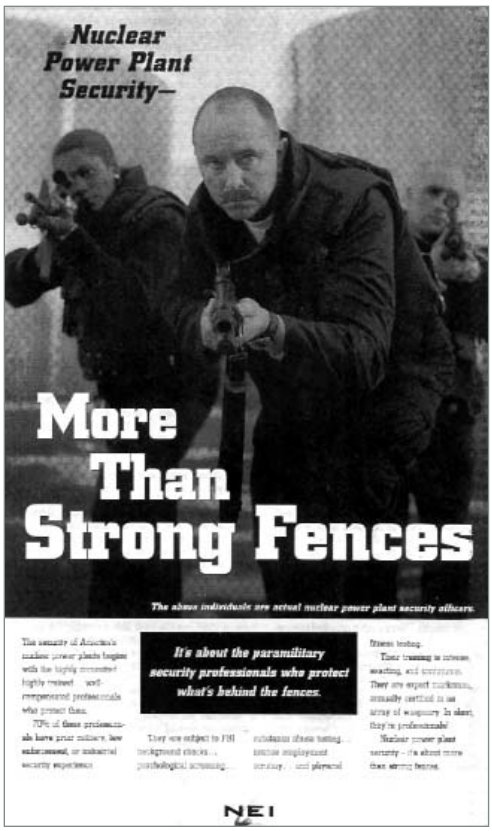
additional security posts, increased vehicle standoff distances," and "tightened facility access controls."

Nuclear plants were given six months to implement the interim measures, which were to be in place by August 31 of last year. It may take as long as two years, though, for NRC inspectors to verify that they have been correctly implemented. Although the upgrades sound impressive, the actual level of protection is hard to gauge because the security testing program, the OSRE, was suspended after September 11 and is only now resuming on a pilot scale.

The NRC has also failed to approve a new DBT that reflects the current terrorist threats. Without significantly tougher requirements, plant operators will continue to lack a clear, consistent, and legally enforceable security performance standard. For instance, the minimum number of armed responders required per shift is believed to have been increased from five to 10, but security managers still do not know how many attackers they are supposed to be defending against.

Until testing has been completed at all nuclear plants, preferably based on a tough new DBT, no one will know how effective the new measures actually are. Tests are important: Security plans that look good on paper are worthless in practice unless the armed responders at nuclear plants are capable of successfully carrying them out in the event of a commando attack. Mock attacks cannot possibly recreate the conditions of real ones, but they can reveal gross deficiencies in guard response.

One of the Nuclear Energy Institute's full-page newspaper ads touting plant security.



The human element

For a successful defense, guards must be well-qualified, physically fit, highly trained, and able to react quickly to contingencies in a combat environment. Boredom, stress, fatigue, and low morale are critical performance factors that must be taken into account.

But the commission has been giving short shrift to the human element. While it has mandated more guards per shift and increased the number of security patrols and posts, it has failed to require plant owners to hire more guards to take up the increased workload. Plant security managers find it more profitable to push the existing security force to the limit than to hire new guards. A recent NRC survey found that 60-hour work weeks were "not infrequent" for security guards at 31 percent of nuclear plant sites. At 11 percent of the sites, 60-hour weeks were "common or routine," and 72-hour work weeks were "not infrequent."

Since September 11, our organizations and others have received numerous complaints from security guards around the country about poor morale, inadequate training, exhaustion from excessive overtime, and poor compensation (below that of the janitorial staff). Most alarming was the sentiment, heard more than once, that guards would not be willing to put their lives on the line, given the pay and treatment they receive from management.

The disturbing picture painted by these guards stands in stark contrast to full-page ads that ran in 2002 in the *Washington Post* and other major newspapers sponsored by the Nuclear Energy Institute (NEI) praising nuclear plant security guards as highly trained paramilitary forces. Resentment about the inaccuracy of NEI's ads was also a recurring theme among the guards who contacted us.

Last September, the Washington, D.C.-based Project on Government Oversight compiled guard complaints from more than 20 percent of U.S. nuclear plants, issuing a highly publicized report that was impossible for the NRC to ignore. As a result, the commission began collecting data from nuclear plants on security guard work weeks—something it had never done before. It even proposed limiting overtime and strengthening training requirements. However, the industry bitterly opposes these initiatives, arguing that guards *like* working six 12-hour shifts in a row. It appears likely that these proposals will get lost in the endless "top-to-bottom" review.

And air attack . . .

In addition to the threat of commando attack, the NRC has taken no action to protect against the ultimate September 11-type threat, a jet aircraft attack, other than to initiate long-term technical studies to evaluate the consequences of air attacks and to require plant operators to plan for events that could "result in damage to large areas of their plants from impacts, explosions, or fires." The commission refuses to consider adding structural features to reactor

sites that might prevent a successful aircraft attack (see "Beamhenge?").

The NRC has also rejected calls by the public and policy-makers to consider the feasibility of directly protecting nuclear plants from air attack by imposing no-fly zones or deploying portable anti-aircraft systems, citing the command-and-control problems inherent in such an approach, the impact on the commercial airline industry, and the risk of accident or collateral damage. These considerations are important, but they must be weighed against the catastrophic consequences of a meltdown and large radiological release, especially at the many nuclear plants in densely populated urban areas—like the controversial Indian Point plant, near New York City. (None of the objections to these defensive measures appear to have prevented them from being taken to protect other buildings; the Pentagon ordered the deployment of heat-seeking anti-aircraft missiles around Washington, D.C. during the recent "code orange" terror alerts.)

Fixing blame

Why can't the NRC deal decisively with urgent threats? The major share of the blame lies with the NRC commissioners, who do not seem to fully appreciate the gravity of the terrorist threat or the devastating consequences that could result from an attack on the facilities they regulate. In a speech in March 2002, Commissioner Edward McGaffigan called nuclear power plants "hard targets by any conceivable definition" and ridiculed those who dared to suggest otherwise.

In June 2002, Commissioner Nils Diaz warned a meeting of the American Nuclear Society that technical progress toward the revival of the nuclear energy option "could be in jeopardy unless unjustified fears of policymakers and the public with regard to . . . the security of these [nuclear power] plants can be addressed." Diaz, who succeeded Meserve as NRC chairman on April 1, also expressed his belief that there would be no significant consequence for the public if a 747 loaded with fuel breached the containment of a nuclear plant—because "America will deliver the necessary responses to protect public health and safety."

Given this sort of wishful thinking, it is little wonder that the commission has let the question of strengthening the DBT languish for well over a year and refuses to impose emergency measures to bolster plant defenses against massive, military-style assaults or aircraft attacks.

Surprisingly, the blame must also be shared by the now-defunct Office of Homeland Security, the Defense Department, and the FBI, all of which have failed to step into the security vacuum created by the NRC's inaction. After September 11, these agencies asked the NRC for its assessment of the consequences of a jet plane attack on a nuclear power plant. While the response is classified, it doesn't take a security clearance to surmise that the commission provided only reassurance.

And one should not forget to blame Congress for failing to enact legislation that could have fixed the most serious nuclear security vulnerabilities, and for creating a department of homeland security that had no authority over nuclear plants.

The other major player is of course the nuclear industry, which has worked to block upgrades of security requirements. The nuclear utilities have always resented having to spend money to prepare for an attack they believe will never occur. Through the NEI, their lobbying arm in Washington, D.C., they have waged a systematic campaign to weaken security regulations.

Before September 11, public observation of meetings between the commission and the industry helped put the brakes on the worst of their proposals, such as their plan to replace the security testing program with an industry-run "self-assessment" program.

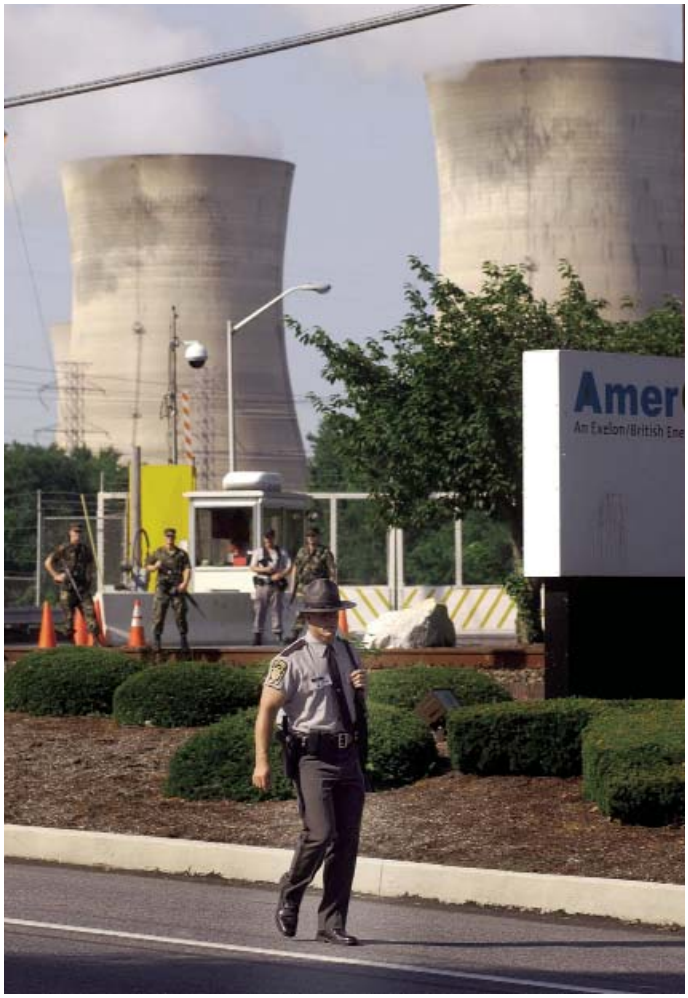
But now the public is no longer welcome at the meetings, even when details of plant security ("safeguards information") are not discussed. All the meetings are now covered under a sweeping but poorly defined new category of restricted information, "sensitive unclassified homeland security information," or "sushi."

The industry is using the new secrecy shield to increase its influence over the regulatory processes. For instance, the interim compensatory measures, although issued by the commission, were the product of multiple closed-door negotiating sessions between the commission and the industry lobby; the NEI actually wrote the document that defined what constituted compliance.

Right now the industry is lobbying hard to significantly weaken any revised DBT. Little wonder that a recent report by the NRC's inspector general found that commission staff believed "that NRC is becoming influenced by private industry and its power to regulate is diminishing."[4]

The NEI has also waged a campaign to convince the public that it has nothing to fear, even if a nuclear plant were attacked by a jet plane fully loaded with fuel. It recently released a summary of a report it commissioned from the Electric Power Research Institute (EPRI), claiming to show that "structures housing reactor fuel at U.S. nuclear power plants would protect against a release of radiation even if struck by a large commercial jetliner."

NEI refused to release the entire report, citing "security considerations," but it was clear from the summary that it had chosen certain assumptions to produce the results it wanted, including a presumed containment wall thickness of four feet—thicker than typical reactor containment walls and domes. EPRI arbitrarily chose an impact speed of 350 miles per hour—well below the nearly 600 miles per hour at which



July 4, 2002: A state police officer patrols the entrance at the Three Mile Island power plant near Harrisburg, Pennsylvania.

ASSOCIATED PRESS

the 767 struck the World Trade Center South Tower. And EPRI ignored the damage that an aircraft could cause to targets outside the containment, like the auxiliary feedwater pumps and the diesel generators.

The insider threat

An individual drives to a nuclear power plant in the United States, obtains an access badge at the security gate, and walks freely through the facility. He takes a rubber hose from an equipment locker and cross-connects the hydrogen gas supply system to the air system. He opens a valve allowing hydrogen gas to flow inside the air system throughout the plant, and within a few minutes, produces combustible levels of hydrogen within the containment building, the auxiliary building, and the turbine building. Using matches, he ignites the explosions and fires that disable the emergency systems needed to cool the reactor core and the systems needed to limit radioactivity releases from the damaged core to the environment.

Sound impossible? Perhaps. But it nearly happened on January 7, 1989, at the H. B. Robinson nuclear plant in South Carolina.[5] An individual made a mistake conducting a test. Luckily, his error was discovered and the buildings were vented of the flammable gas mixture before disaster struck. But what prevents workers from accomplishing by intent that which nearly happened by mistake—sabotage from the inside?

Three conditions are supposed to be met for an individual to have unescorted access at a nuclear power plant:

- A background investigation—to verify identity, employment history, education history, credit history, criminal history, military service, and character and reputation;
- A psychological assessment, to identify any characteristics with potential bearing on the individual's trustworthiness and reliability; and
- Continuing behavioral observation, to detect any changes that might indicate a propensity for sabotage.[6]

Outgoing NRC Chairman Richard Meserve conceded that although these requirements are important, they are not always met. As Meserve wrote to Homeland Security Director Tom Ridge, "enhancing access control may be one of the most effective means of preventing a successful attack."[7]

Background investigations are spotty. Criminal history checks are performed by the submission of fingerprint cards to the FBI's National Crime Information Center, but results are not timely. The NRC has accelerated the turnaround time for the checks since September 11, but individuals continue to gain access by lying about their criminal records. Workers at the Fermi, Perry, and Oconee nuclear plants have recently lost their unescorted access privileges after FBI checks revealed criminal histories.[8]

In addition to being slow, background checks fail to delve deeply enough. According to Meserve:

"U.S. citizens are currently accounted for better than foreign applicants due to lack of information (e.g., credit history and criminal history) or unwillingness of the [foreign] country to provide such information. Licensees determine access to the facilities regarding foreign applicants on a 'best effort' basis."[9]

In other words, despite fears that foreign terrorist cells may be operating within the United States, background checks for nuclear workers essentially stop at the border. Terrorists could probably get unescorted access to U.S. nuclear plants if they have no traffic arrests or shoplifting convictions.

The questionable value of the psychological assessment screening tool is reflected in the Carl Drega case. Drega was killed in a police shootout in August 1997 after a series of shootings in New England that left four others dead. Police later found bomb-making materials in his home. Drega had had unescorted access when he worked at the Vermont Yankee, Pilgrim, and Indian Point 3 nuclear plants between 1992 and 1997. He had applied for unescorted access to the Seabrook nuclear plant, too, but the plant owner denied his request. The NRC determined that Seabrook's owner would have granted him unescorted access if he had not parked his mobile home on Seabrook property and attempted to live there.[10]

The final protection against insider sabotage is continuing observation. Supervisors are trained to detect changes in behavior patterns that

might be symptoms of mental stress caused by problems on the job or at home. Upon detection of any such changes, supervisors are instructed to interact with the worker and suggest counseling. It seems doubtful that if a supervisor identified a saboteur midplot, a suggestion to seek counseling would make much difference.

Contrast feckless continuing behavior observation against the announcement that would be read over the public address system at the Callaway nuclear plant in Missouri if an insider were suspected of trying to sabotage the facility:

"The Callaway Plant has received a Credible Security Threat. Included in this threat is information indicating that someone at the plant may be involved in an effort to cause damage to the plant. All personnel who have a work-related need to enter a card reader area inside the Protected Area must be accompanied by another person. . . . The two persons do not need to have the same skills but must have access to the same areas. The purpose is to ensure observation of all personnel in these areas."[11]

Adoption of a "two-person rule" would make it harder for the lone saboteur. Card readers restrict access to vital areas within the plant. Most areas of a plant are not classified as vital, but the control room, the emergency diesel generator rooms, and other areas containing essential equipment are. Observation of all personnel in vital areas might be a prudent anti-sabotage measure, but observation is not routine. Nuclear plants have plenty of security cameras, but most of them are trained on perimeter fences. Workers normally have both unescorted and unmonitored access to vital areas.

To turn Meserve's wish for enhanced access control into reality, the NRC should expeditiously:

- Require criminal history checks to be completed *before* individuals gain unescorted access.
- Require foreign nationals to have background checks comparable to those required of U.S. citizens *before* gaining unescorted access to nuclear facilities.
- Require the two-person rule for entry into infrequently accessed vital areas and require security camera monitoring of all other vital areas.

The nuclear industry should be expected to resist these security upgrades. In June 2000, Exelon, which owns 17 nuclear plants, proposed that the NRC "eliminate the requirement to protect against the insider threat."[12]

Public awareness

Better security at sensitive facilities is needed more than ever, but the NRC and the nuclear industry have spent most of their time arguing against improvements. Some of those arguments have been extraordinary—for example, that Chernobyl wasn't so bad. Recent commentaries by a group of prominent nuclear industry figures made that assertion and even went so far as to claim that the release of radiation would be good for the public: "Data show detrimental health effects and biological functions when organisms are 'protected' from . . . radiation."[13]

But imagine if the public were told that more than 100 massive radiological weapons—"dirty bombs" on an incomprehensible scale—had been pre-emplaced in the United States, each capable of rendering an area the size of Pennsylvania uninhabitable for decades. Imagine further that the public learned that despite all the hype about homeland security, a powerful industry and its captured regulatory agency had succeeded in blocking security measures that would prevent those weapons from being used against the U.S. population. But one needn't imagine—it's the NRC's latest dirty little secret. ⚛

1. See 10 CFR 73.1 and 50.13; NRC PG&E Diablo Canyon decision ALAB-653, September 9, 1981; SECY–76-242C.

2. Daniel Hirsch, "The NRC: What, Me Worry?" *Bulletin of the Atomic Scientists*, January/February 2002; "Protecting Reactors from Terrorists," Daniel Hirsch, Stephanie Murphy, and Bennett Ramberg, *Bulletin,* August/September 1986; "The Truck Bomb and Insider Threats to Nuclear Facilities," in Paul Leventhal, ed., *Preventing Nuclear Terrorism* (Lexington, Mass.: Lexington Books, 1987); and "Nuclear Terrorism: A Growing Threat," A Report to the Safeguards and Security Subcommittee, Advisory Committee on Reactor Safeguards, U.S. Nuclear Regulatory Commission (hereafter "NRC"), by Daniel Hirsch, Stephanie Murphy, and Bennett Ramberg, May 7, 1985, reprinted in monograph series, Stevenson Program on Nuclear Policy, University of California Santa Cruz, SPNP-85-F-1.

3. "Differing Professional View Regarding NRC Abandoning its Only Counter-Terrorism Program," NRC memo from Capt. David Orrik to Samuel Collins, August 7, 1998.

4. NRC, Office of the Inspector General, "OIG 2002 Survey of NRC's Safety Culture and Climate," December 11, 2002.

5. NRC, Preliminary Notification of Event or Unusual Occurrence PNO-II-89-04, "Flammable Mixture of Hydrogen in H. B. Robinson's Station Air System," January 9, 1989.

6. Section 73.56, "Personnel Access Authorization Requirements for Nuclear Power Plants," Title 10, "Energy," Code of Federal Regulations.

7. Richard A. Meserve, Chairman, NRC, letter dated September 5, 2002, to Gov. Tom Ridge, Office of Homeland Security.

8. William T. O'Connor Jr., Vice President, Nuclear Generation, Detroit Edison, letter dated November 14, 2001, to NRC, "Safeguards Event Report (SER) No. 01-S01"; Cynthia D. Pederson, Director, Division of Reactor Safety, NRC, letter dated September 26, 2002, to William R. Kanda, Vice President, Nuclear, Perry, FirstEnergy Nuclear Operating Company, "Office of Investigations Report No. 3-2001-059"; W. R. McCollum, Jr., Vice President, Duke Energy, letter dated April 9, 2002, to NRC, "Oconee Nuclear Station/Docket Nos. 50-269, -270, -287/Licensee Event Report 269/2002-S01, Revision 0/Problem Investigation Process No.: O-02-1301."

9. Richard A. Meserve, Chairman, NRC, letter dated March 4, 2002, to Cong. Edward J. Markey, U.S. House of Representatives.

10. L. Joseph Callan, Executive Director for Operations, NRC, memorandum dated May 20, 1998, to Chairman and Commissioners, NRC, SECY-98-110, "Report on Inspection and Programmatic Findings Relating to the Carl C. Drega Incident."

11. Ameren UE, Emergency Implementing Procedure EIP-ZZ-SK001, "Response to Security Events," Revision 000, June 27, 2002.

12. ComEd, Presentation Slides, "Meeting with NRC Office of Research–Unnecessary Regulatory Burden," June 14, 2000.

13. Douglas M. Chapin et al., "Policy Forum," *Science,* September 20, 2002; Chapin et al., letters, *Science,* January 10, 2003.