Order Code RL34331

# CRS Report for Congress

## Nuclear Power Plant Security and Vulnerabilities

**January 18, 2008**

Mark Holt and Anthony Andrews
Specialists in Energy Policy
Resources, Science, and Industry Division


Prepared for Members and
Committees of Congress

# Nuclear Power Plant Security and Vulnerabilities


## Summary

The physical security of nuclear power plants and their vulnerability to deliberate acts of terrorism was elevated to a national security concern following the events of September 11, 2001.

Title VI of the Energy Policy Act of 2005 regarding nuclear security amended the Atomic Energy Act with the addition of new provisions for security evaluations and rulemaking to revise the "Design Basis Threat." The act included provisions for fingerprinting and criminal background checks of security personnel, their use of firearms, and the unauthorized introduction of dangerous weapons. The designation of facilities subject to enforcement of penalties for sabotage expanded to include treatment and disposal facilities.

As part of security response evaluations, the act requires the Nuclear Regulatory Commission (NRC) to conduct "force-on-force" security exercises at nuclear power plants at least once every three years, and revise the "design-basis threat" to consider a wider variety of potential attacks.

The NRC has strengthened its regulations on nuclear power plant security, but critics contend that implementation by the industry has been too slow and that further measures are needed. Vulnerability to a deliberate aircraft crash remains an outstanding issue, as the latest NRC rulemaking addresses only newly designed plants. Shortcomings in the performance of security contractors has drawn the attention of Congress.

This report will be updated as events warrant.

## Contents

# Nuclear Power Plant Security and Vulnerabilities

## Background

Physical security at nuclear power plants concerns the threat of radiological sabotage, a deliberate act against a plant that could directly or indirectly endanger public health and safety through exposure to radiation. Out of Cold War concerns, the Nuclear Regulatory Commission (NRC) in 1967 instituted a provision that nuclear plants are not required to protect against an attack directed by an "enemy of the United States."[1] This principle was reflected in the initial "Design Basis Threat" (DBT) in the late 1970s, describing potential attacks that nuclear plants must prepare for, including the number of attackers, their training, and the weapons and tactics they are capable of employing.

Following the September 11, 2001, attacks on the Pentagon and the World Trade Center, the Nuclear Regulatory Commission (NRC) began a "top-to-bottom" review of its nuclear power plant security requirements. On February 25, 2002, the agency issued "interim compensatory security measures" to deal with the "generalized high-level threat environment" that continued to exist, and on January 7, 2003, it issued regulatory orders that tightened nuclear plant access. On April 29, 2003, NRC issued three orders to restrict security officer work hours, establish new security force training and qualification requirements, and increase the DBT that nuclear security forces must be able to defend against.

In the Energy Policy Act of 2005 (EPACT), Congress imposed a statutory requirement on the NRC to initiate rulemaking for revising the design basis threat.[2] The DBT, a classified document, describes general characteristics of adversaries that nuclear plants and nuclear fuel cycle facilities must defend against, including radiological sabotage and theft of strategic special nuclear material. EPACT required NRC to consider 12 factors in revising the DBT, including but not limited to an assessment of various terrorist threats, sizable explosive devices and modern weapons, attacks by persons with sophisticated knowledge of facility operations, and attacks on spent fuel shipments.

Critics of NRC's security measures had demanded both short-term regulatory changes and legislative reforms. A fundamental concern was the nature of the DBT,

---

[1] It was feared that Cuba might launch an attack on Florida reactors. Government Accountability Office, *Nuclear Power Plants — Efforts Made to Upgrade Security, but the Nuclear Regulatory Commission's Design Basis Threat Process Should Be Improved* (GAO-06-388), March 2006, p. 2. Regulations at 10 CFR 50.13.

[2] P.L. 109-58, Title VI, Subtitle D — Nuclear Security (Secs. 651-657). Sec. 651 adds Atomic Energy Act Sec. 170E. Design Basis Threat Rulemaking.

which critics contended should be increased to include a number of separate, coordinated attacks. In revising the DBT in 2003, the NRC indicated that a private security force employed by a nuclear power plant cannot reasonably be expected to defend against all threats — for example, airborne attacks. The prospect of a highjacked airliner repeating a 9/11-like airborne attack on a nuclear power plant continues to draw concern.

Critics also pointed out that licensees are required to employ only a minimum of five security personnel on duty per plant, which they argue is not enough for the job.[3] Nuclear spokespersons responded that the actual security force for the nation's 65 nuclear plant sites numbers more than 5,000, an average of about 75 per site (covering multiple shifts). Nuclear plant security forces are also supposed to be aided by local law enforcement officers if an attack occurs.

## Plant Physical Security

Regulations in place prior to the September 11 attacks (10 C.F.R. 73 — Physical Protection of Plants and Materials) required all NRC-licensed commercial nuclear power plants to have a series of physical barriers and a trained security force. The plant sites were divided into three zones: an "owner-controlled" buffer region, a "protected area," and a "vital area." Access to the protected area was restricted to a portion of plant employees and monitored visitors, with stringent access barriers. The vital area was further restricted, with additional barriers and access requirements. The security force had to comply with NRC requirements on pre-hiring investigations and training.[4]

The NRC proposed to amend the security regulations and add new security requirements that would codify the series of four orders supplementing the DBT issued after 9/11.[5] One of NRC's regulatory orders (April 2003) changed the DBT to "represent the largest reasonable threat against which a regulated private guard force should be expected to defend under existing law," according to the NRC announcement.[6] NRC approved its final rule amending the DBT (10 C.F.R. Part 73.1) on January 29, 2007.[7] As directed by the Energy Policy Act, the final rule imposed

---

[3] 10 C.F.R. 73.55 (h)(3) states: "The total number of guards, and armed, trained personnel immediately available at the facility to fulfill these response requirements shall nominally be ten (10), unless specifically required otherwise on a case by case basis by the Commission; however, this number may not be reduced to less than five (5) guards."

[4] General NRC requirements for nuclear power plant security can be found in 10 C.F.R. 73.55.

[5] *Federal Register*, October 26, 2006 (vol. 71, no. 207), NRC, Power Reactor Security Requirements, Proposed Rule.

[6] *Federal Register*, May 7, 2003 (vol. 68, no. 88). NRC, All Operating Power Reactor Licensees; Order Modifying Licenses.

[7] *Federal Register*, March 19, 2007 (vol. 72, no. 52), NRC, Design Basis Threat, Final Rule, pp. 12705-12727.

the security requirements of the April 2003 order, making the DBT orders generically applicable.

## Design Basis Threat

The design basis threat is used by NRC licensees as the basis for implementing defensive strategies of a specific nuclear plant site through security plans, safeguards contingency plans, and guard training and qualification plans. Although specific details of the revised DBT were not released to the public, in general the final rule

- clarifies that physical protection systems are required to protect against diversion and theft of fissile material;
- expands the assumed capabilities of adversaries to operate as one or more teams and attack from multiple entry points;
- assumes that adversaries are willing to kill or be killed and are knowledgeable about specific target selection;
- expands the scope of vehicles that licensees must defend against to include water vehicles and land vehicles beyond four-wheel-drive type;
- revises the threat posed by an insider to be more flexible in scope; and
- adds a new mode of attack from adversaries coordinating a vehicle bomb assault with another external assault.

In 2006, the Government Accountability Office (GAO) reviewed the upgrades in nuclear plant security and found a generally logical and well-defined process.[8] GAO found NRC staff trained in threat assessment who monitor information provided by intelligence agencies and screen the information to evaluate particular terrorist capabilities for inclusion in the DBT. However, the NRC produced a revised DBT that generally, but not always, corresponded to the threat assessment staff's original recommendations.

The DBT final rule excluded aircraft attacks, which raised considerable controversy. In approving the rule, NRC rejected a petition from the Union of Concerned Scientists to require that nuclear plants be surrounded by aircraft barriers made of steel beams and cables (the so-called "beamhenge" concept). Critics of the rule charged that deliberate aircraft crashes were a highly plausible mode of attack, given the events of 9/11. However, NRC contended that power plants were already required to mitigate the effects of aircraft crashes and that "active protection against airborne threats is addressed by other federal organizations, including the military."[9] Additional NRC action on aircraft threats is discussed below.

---

[8] GAO-06-388

[9] NRC, "NRC Approves Final Rule Amending Security Requirements," News Release No. 07-012, January 29, 2007.

## Force-On-Force Exercises

EPACT codified an NRC requirement that each nuclear power plant conduct security exercises every three years to test its ability to defend against the design basis threat. In these "force-on-force" exercises, monitored by NRC, an adversary force from outside the plant attempts to penetrate the plant's vital area and damage or destroy key safety components. Participants in the tightly controlled exercises carry weapons modified to fire only blanks and laser bursts to simulate bullets, and they wear laser sensors to indicate hits. Other weapons and explosives, as well as destruction or breaching of physical security barriers, may also be simulated. While one squad of the plant's guard force is participating in a force-on-force exercise, another squad is also on duty to maintain normal plant security. Plant defenders know that a mock attack will take place sometime during a specific period of several hours, but they do not know what the attack scenario will be. Multiple attack scenarios are conducted over several days of exercises.

In response to the growing emphasis on security, NRC established the Office of Nuclear Security and Incident Response on April 7, 2002. The office centralizes security oversight of all NRC-regulated facilities, coordinates with law enforcement and intelligence agencies, and handles emergency planning activities. Force-on-force exercises are an example of the office's responsibilities.

Full implementation of the force-on-force program began in late 2004. Standard procedures and other requirements have been developed for using the force-on-force exercises to evaluate plant security and as a basis for taking regulatory enforcement action. Many tradeoffs are necessary to make the exercises as realistic and consistent as possible without endangering participants or regular plant operations and security.

NRC required the nuclear industry to develop and train a "composite adversary force" comprising security officers from many plants to simulate terrorist attacks in the force-on-force exercises. However, in September 2004 testimony, GAO criticized the industry's selection of a security company that guards about half of U.S. nuclear plants, Wackenhut, to also provide the adversary force. In addition to raising "questions about the force's independence," GAO noted that Wackenhut had been accused of cheating on previous force-on-force exercises by the Department of Energy.[10] Exelon terminated its security contracts with Wackenhut in late 2007 after guards at the Peach Bottom reactor in York County, Pennsylvania, were discovered sleeping while on duty.[11] EPACT requires NRC to "mitigate any potential conflict of interest that could influence the results of a force-on-force exercise, as the Commission determines to be necessary and appropriate."

---

[10] GAO. "Nuclear Regulatory Commission: Preliminary Observations on Efforts to Improve Security at Nuclear Power Plants." Statement of Jim Wells, Director, Natural Resources and Environment to the Subcommittee on National Security, Emerging Threats, and International Relations, House Committee on Government Reform. September 14, 2004. p. 14.

[11] *Washington Post*, "Executive Resigns in Storm Over Sleeping Guards," January 10, 2008.

## Emergency Response

After the 1979 accident at the Three Mile Island nuclear plant near Harrisburg, PA, Congress required that all nuclear power plants be covered by emergency plans. NRC requires that within an approximately 10-mile Emergency Planning Zone (EPZ) around each plant, the operator must maintain warning sirens and regularly conduct evacuation exercises monitored by NRC and the Federal Emergency Management Agency (FEMA). In light of the increased possibility of terrorist attacks that, if successful, could result in release of radioactive material, critics have renewed calls for expanding the EPZ to include larger population centers.

The release of radioactive iodine during a nuclear incident is a particular concern, because iodine tends to concentrate in the thyroid gland of persons exposed to it. Emergency plans in many states include distribution of iodine pills to the population within the EPZ. Taking non-radioactive iodine before exposure would prevent absorption of radioactive iodine but would afford no protection against other radioactive elements. In 2002, NRC began providing iodine pills to states requesting them for populations within the 10-mile EPZ.

# Nuclear Plant Vulnerability

The major concerns in operating a nuclear power plant are controlling the nuclear chain reaction and assuring that the reactor core does not lose its coolant and "melt down" from the heat produced by the radioactive fission products within the fuel rods. U.S. plants are designed and built to prevent dispersal of radioactivity, in the event of an accident, by surrounding the reactor in a steel-reinforced concrete containment structure, which represents an intrinsic safety feature. Two major accidents have taken place in power reactors, at Three Mile Island (TMI) in 1979 and at Chernobyl in the Soviet Union in 1986. Although both accidents resulted from a combination of operator error and design flaws, TMI's containment structure effectively prevented a major release of radioactivity from a fuel meltdown caused by the loss of coolant. In the Chernobyl accident, the reactor's protective barriers were breached when an out-of-control nuclear reaction led to a fierce graphite fire that caused a significant part of the radioactive core to be blown into the atmosphere.

## Vulnerability from Air Attack

Nuclear power plants were designed to withstand hurricanes, earthquakes, and other extreme events. But deliberate attacks by large airliners loaded with fuel, such as those that crashed into the World Trade Center and Pentagon, were not analyzed when design requirements for today's reactors were determined.[12] A taped interview shown September 10, 2002, on Arab TV station al-Jazeera, which contained a statement that Al Qaeda initially planned to include a nuclear plant in its list of 2001 attack sites, intensified concern about aircraft crashes.

---

[12] Meserve, Richard A., NRC Chairman, "Research: Strengthening the Foundation of the Nuclear Industry," Speech to Nuclear Safety Research Conference, October 29, 2002.

In light of the possibility that an air attack might penetrate the containment building of a nuclear plant, some interest groups have suggested that such an event could be followed by a meltdown and widespread radiation exposure. Nuclear industry spokespersons have countered by pointing out that relatively small, low-lying nuclear power plants are difficult targets for attack, and have argued that penetration of the containment is unlikely, and that even if such penetration occurred it probably would not reach the reactor vessel. They suggest that a sustained fire, such as that which melted the steel support structures in the World Trade Center buildings, would be impossible unless an attacking plane penetrated the containment completely, including its fuel-bearing wings. According to former NRC Chairman Nils Diaz, NRC studies "confirm that the likelihood of both damaging the reactor core and releasing radioactivity that could affect public health and safety is low."[13]

NRC proposes to amend its regulations with a new rule that would require newly designed power reactor facilities to take into account the potential effects of the impact of a large, commercial aircraft.[14] The proposed rule would only affect new reactor designs not previously certified by NRC.[15] Westinghouse submitted changes in the design of its AP1000 reactor to NRC on May 29, 2007, proposing to line the inside and outside of the reactor's concrete containment structure with steel plates to increase resistance to aircraft penetration.[16]

## Spent Fuel Storage

When no longer capable of sustaining a nuclear chain reaction, "spent" nuclear fuel is removed from the reactor and stored in a pool of water in the reactor building and at some sites later transferred to dry casks on the plant grounds. Because both types of storage are located outside the reactor containment structure, particular concern has been raised about the vulnerability of spent fuel to attack by aircraft or other means. If terrorists could breach a spent fuel pool's concrete walls and drain the cooling water, the spent fuel's zirconium cladding could overheat and catch fire.

The National Academy of Sciences (NAS) released a report in April 2005 that found that "successful terrorist attacks on spent fuel pools, though difficult, are possible," and that "if an attack leads to a propagating zirconium cladding fire, it could result in the release of large amounts of radioactive material." NAS recommended that the hottest spent fuel be interspersed with cooler spent fuel to reduce the likelihood of fire, and that water-spray systems be installed to cool spent fuel if pool water were lost. The report also called for NRC to conduct more analysis of the issue and consider earlier movement of spent fuel from pools into dry

---

[13] Letter from NRC Chairman Nils J. Diaz to Secretary of Homeland Security Tom Ridge, September 8, 2004.

[14] *Federal Register*, October 3, 2007 (vol. 72, no. 191), Consideration of Aircraft Impacts for New Nuclear Power Reactor Designs.

[15] NRC, "NRC Proposes Adding Plane Crash Security Assessments to New Reactor Design Certification Requirements," News Release No. 07-053, April 24, 2007.

[16] MacLachlan, Ann, "Westinghouse Changes AP1000 Design to Improve Plane Crash Resistance," Nucleonics Week, June 21, 2007.

storage.[17] The FY2006 Energy and Water Development Appropriations Act (P.L. 109-103, H.Rept. 109-275) provided $21 million for NRC to carry out the site-specific analyses recommended by NAS.

NRC has long contended that the potential effects of terrorist attacks are too speculative to include in environmental studies for proposed spent fuel storage and other nuclear facilities. However, the U.S. Court of Appeals for the 9th Circuit ruled in June 2006 that terrorist attacks must be included in the environmental study of a dry storage facility at California's Diablo Canyon nuclear plant. NRC reissued the Diablo Canyon study May 29, 2007, to comply with the court ruling, but it did not include terrorism in other recent environmental studies.[18]

## Regulatory and Legislative Proposals

After video recordings of inattentive security officers at the Peach Bottom (PA) nuclear power plant were aired on local television, an NRC inspection in late September 2007 confirmed that there had been multiple occasions on which multiple security officers were inattentive.[19] However, after a follow-up inspection into security issues at the Peach Bottom plant, the NRC concluded that the plant's security program had not been significantly degraded as a result of the guards' inattentiveness. NRC issued a bulletin December 12, 2007, requiring all nuclear power plants to provide written descriptions of their "managerial controls to deter and address inattentiveness and complicity among licensee security personnel."

The House Committee on Energy and Commerce announced January 7, 2008, that it would conduct a comprehensive review of the NRC's oversight operations.[20] "The NRC's stunning failure to act on credible allegations of sleeping security guards, coupled with its unwillingness to protect the whistleblower who uncovered the problem, raises troubling questions," said Representative John D. Dingell, Chairman of the Committee.

---

[17] National Academy of Sciences, Board on Radioactive Waste Management, Safety and Security of Commercial Spent Nuclear Fuel Storage, Public Report (online version), released April 6, 2005.

[18] Beattie, Jeff, "NRC Takes Two Roads on Terror Review Issue," The Energy Daily, February 27, 2007.

[19] NRC, *NRC Commences Follow-up Security Inspection at Peach Bottom*, November 5, 2007 [http://www.nrc.gov/reading-rm/doc-collections/news/2007/07-057.i.html].

[20] Committee on Energy and Commerce, *Energy and Commerce Committee to Probe Breakdowns in NRC Oversight*, January 7, 2008 [http://energycommerce.house.gov/Press_110/110nr149.shtml].