Nuclear Power Plant Security and Vulnerabilities

Mark Holt
Specialist in Energy Policy

Anthony Andrews
Specialist in Energy and Energy Infrastructure Policy

March 18, 2009

Congressional Research Service
7-5700
www.crs.gov
RL34331

CRS Report for Congress
Prepared for Members and Committees of Congress

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 September 11, 2001 attacks. Since then, Congress has repeatedly focused oversight and legislative attention on nuclear power plant security requirements established and enforced by the Nuclear Regulatory Commission (NRC).

The Energy Policy Act of 2005 (P.L. 109-58) imposed specific criteria for NRC to consider in revising the "Design Basis Threat" (DBT), which specifies the maximum severity of potential attacks that a nuclear plant's security force must be capable of repelling. In response to the legislative mandate, NRC revised the DBT (10 C.F.R. Part 73.1) on April 18, 2007. Among other changes, the revisions expanded the assumed capabilities of adversaries to operate as one or more teams and attack from multiple entry points.

To strengthen nuclear plant security inspections, the Energy Policy Act of 2005 act required NRC to conduct "force-on-force" security exercises at nuclear power plants at least once every three years. In these exercises, a mock adversary force from outside a nuclear plant attempts to penetrate the plant's vital area and simulate damage to key safety components. The first three-year cycle of force-on-force exercises was completed for all U.S. nuclear plants at the end of calendar year 2007. During that period, 172 force-on-force exercises were conducted (an average of three per site), and 10 security inadequacies were cited. Two of the exercises, both in 2007, resulted in simulated damage or destruction of a vital target by the adversary team. In both cases, NRC ordered corrective actions and conducted follow-up exercises to confirm the improvements.

The Energy Policy Act also 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 was expanded to include treatment and disposal facilities.

Nuclear power plant vulnerability to deliberate aircraft crashes has been a continuing issue. After much consideration, NRC voted February 17, 2009, to require all new nuclear power plants to incorporate design features that would ensure that, in the event of a crash by a large commercial aircraft, the reactor core would remain cooled or the reactor containment would remain intact, and radioactive releases would not occur from spent fuel storage pools.

NRC rejected proposals that existing reactors also be required to protect against aircraft crashes, such as by adding large external steel barriers. However, NRC did impose some additional requirements related to aircraft crashes on all reactors, both new and existing, after the 9/11 attacks. In 2002, NRC ordered all nuclear power plants to develop strategies to mitigate the effects of large fires and explosions that could result from aircraft crashes or other causes. An NRC regulation on fire mitigation strategies, along with requirements that reactors establish procedures for responding to specific aircraft threats, was approved December 17, 2008.

Other ongoing nuclear plant security issues include the vulnerability of spent fuel pools, which hold highly radioactive nuclear fuel after its removal from the reactor, standards for nuclear plant security personnel, and nuclear plant emergency planning. NRC's December 2008 security regulations addressed some of those concerns and included a number of other security enhancements.

Contents

Contacts

Overview of Reactor Security

Physical security at nuclear power plants involves 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. The Nuclear Regulatory Commission (NRC) establishes security requirements at U.S. commercial nuclear power plants based on its assessment of plant vulnerabilities to, and the consequences of, potential attacks. The stringency of NRC's security requirements and its enforcement program have been a significant congressional issue, especially since the September 11, 2001, terrorist attacks on the United States.

Nuclear plant security measures are designed to protect three primary areas of vulnerability: controls on the nuclear chain reaction, cooling systems that prevent hot nuclear fuel from melting even after the chain reaction has stopped, and storage facilities for highly radioactive spent nuclear fuel. 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.

NRC requires commercial nuclear power plants to have a series of physical barriers and a trained security force, under regulations already in place prior to the 9/11 attacks (10 C.F.R. 73—Physical Protection of Plants and Materials). The plant sites are divided into three zones: an "owner-controlled" buffer region, a "protected area," and a "vital area." Access to the protected area is restricted to a portion of plant employees and monitored visitors, with stringent access barriers. The vital area is further restricted, with additional barriers and access requirements. The security force must comply with NRC requirements on pre-hiring investigations and training.[1]

A fundamental concept in NRC's physical security requirements is the design basis threat (DBT), which establishes the severity of the potential attacks that a nuclear plant's security force must be capable of repelling. The DBT includes such characteristics as the number of attackers, their training, and the weapons and tactics they could use. Specific details are classified. Critics of nuclear plant security have contended that the DBT should be strengthened to account for potentially larger and more sophisticated terrorist attacks.

Reactor vulnerability to deliberate aircraft crashes has also been a major concern since 9/11. Most existing nuclear power plants were not specifically designed to withstand crashes from large jetliners, although analyses differ as to the damage that could result. NRC has determined that commercial aircraft crashes are beyond the DBT but voted in February 2009 to require that new reactor designs be able to withstand such crashes without releasing radioactivity. Nuclear power critics have called for retrofits of existing reactors as well.

Since the 9/11 attacks, NRC and Congress have taken action to increase nuclear power plant security. NRC issued a series of security measures beginning in 2002, including a strengthening of the DBT and establishing the Office of Nuclear Security and Incident Response (NSIR). The office centralizes security oversight of all NRC-regulated facilities, coordinates with law enforcement and intelligence agencies, and handles emergency planning activities. In 2004, NRC implemented a program to conduct "force on force" security exercises overseen by NSIR at each nuclear power plant at least every three years. The Energy Policy Act of 2005 (P.L. 109-58) required NRC to further strengthen the DBT, codified the force-on-force program, and established

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

a variety of additional nuclear plant security measures. In December 2008, NRC approved a series of security regulations that require power plants to prepare cyber security plans, develop strategies for dealing with the effects of aircraft crashes, strengthen access controls, improve training for security personnel, and take other new security measures.

Design Basis Threat

The design basis threat describes general characteristics of adversaries that nuclear plants and nuclear fuel cycle facilities must defend against to prevent radiological sabotage and theft of strategic special nuclear material. NRC licensees use the DBT 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.

General requirements for the DBT are prescribed in NRC regulations,[2] while specific attributes of potential attackers, such as their weapons and ammunition, are contained in classified adversary characteristics documents (ACDs).

Fundamental policies on nuclear plant security threats date back to the Cold War. In 1967, the Atomic Energy Commission (AEC) instituted a rule that nuclear plants are not required to protect against an attack directed by an "enemy of the United States."[3] That so-called "Enemy of the State Rule" specifies that nuclear power plants are

> not required to provide for design features or other measures for the specific purpose of protection against the effects of (a) attacks and destructive acts, including sabotage, directed against the facility by an enemy of the United States, whether a foreign government or other person, or (b) use or deployment of weapons incident to U.S. defense activities.[4]

The Nuclear Regulatory Commission (NRC), the AEC's successor regulatory agency, says that the rule "was primarily intended to make clear that privately-owned nuclear facilities were not responsible for defending against attacks that typically could only be carried out by foreign military organizations."[5] NRC's initial DBT, established in the late 1970s, was intended to be consistent with the enemy of the state rule, which remains in effect.

However, the 9/11 attacks drew greater attention to the potential severity of credible terrorist threats. Following the attacks, NRC evaluated the extent to which nuclear plant security forces should be able to defend against such threats, and ordered a strengthening of the DBT, along with other security measures, on April 29, 2003. That order 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]

---

[2] 10 C.F.R. § 73.1.

[3] 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.

[4] 10 C.F.R. § 50.13. Attacks and destructive acts by enemies of the United States; and defense activities.

[5] Nuclear Regulatory Commission, "Design Basis Threat," 72 *Federal Register* 12714, March 19, 2007.

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

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.[7] EPACT required NRC to consider 12 factors in revising the DBT, such as 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.

NRC approved its final rule amending the DBT (10 C.F.R. Part 73.1) on January 29, 2007, effective April 18, 2007.[8] 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.

The DBT final rule excluded aircraft attacks, a decision that 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.

NRC Commissioners in January 2009 rejected a proposal by the NRC staff to strengthen the classified portion of the DBT to include additional capabilities by potential attackers, according to news reports. The staff proposal lost in a 2-2 vote, with one commissioner position currently vacant. In an interview afterward, NRC Chairman Dale Klein said the vote could be reconsidered after completion of an ongoing interagency study.[10]

Critics of NRC's security regulations have 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.[11] Nuclear spokespersons responded that the actual security force for the nation's 65 nuclear

[7] 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.

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

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

[10] Jeff Beattie, "NRC Chairman Questions Case for Tougher DBT," *Energy Daily*, February 17, 2009, p. 1.

[11] 10 C.F.R. 73.55 (h)(3) states: "The total number of guards, and armed, trained personnel immediately available at the (continued...)

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.

Large Aircraft Crashes

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] Concern about aircraft crashes was intensified by a taped interview shown September 10, 2002, on the 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.

In light of the possibility that an air attack might penetrate the containment structure of a nuclear plant or a spent fuel storage facility, some interest groups have suggested that such an event could be followed by a meltdown or spent fuel fire 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 proposed in October 2007 to amend its regulations to require newly designed power reactors to take into account the potential effects of the impact of a large commercial aircraft. [14] As discussed in the previous section, NRC considers an aircraft attack to be beyond the design basis threat that plants must be able to withstand, so the requirements of the proposed rule were intended to provide an additional margin of safety. The proposed rule would affect only new reactor designs not previously certified by NRC, because the previous designs were still considered adequately safe. Nevertheless, Westinghouse submitted changes in the certified 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.[15]

(...continued)

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."

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

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

Under NRC's 2007 proposed rule, applicants for new certified designs or for new reactor licenses using uncertified designs would have been required to assess the effects that a large aircraft crash would have on the proposed facilities. Each applicant would then describe how the plant's design features, capabilities, and operations would avoid or mitigate the effects of such a crash, particularly on core cooling, containment integrity, and spent fuel storage pools.

In response to comments, the NRC staff proposed in October 2008 that the aircraft impact assessments be conducted by all new reactors, including those using previously certified designs.[16] The NRC Commissioners, in a 3-1 vote, approved the change February 17, 2009, and added specific design requirements that all new reactors would have to meet:[17]

> Each applicant subject to this section shall perform a design-specific assessment of the effects on the facility of the impact of a large, commercial aircraft. Using realistic analyses, the applicant shall identify and incorporate into the design those design features and functional capabilities to show that, with reduced use of operator actions:
>
> (A) the reactor core remains cooled, or the containment remains intact; and
>
> (B) spent fuel cooling or spent fuel pool integrity is maintained.

As noted above, NRC rejected proposals that existing reactors—in addition to new reactors—be required to protect against aircraft crashes, such as by adding "beamhenge" barriers. However, NRC did impose some additional requirements related to aircraft crashes on all reactors after the 9/11 attacks. In 2002, NRC ordered all nuclear power plants to develop strategies to mitigate the effects of large fires and explosions that could result from aircraft crashes or other causes.[18] As part of a broad security rulemaking effort, NRC proposed in October 2006 to incorporate the 2002 order on fire and explosion strategies into its security regulations (10 CFR Part 73).[19] In response to comments, NRC published a supplemental proposed rule in April 2008 to move the fire and explosion requirements into its reactor licensing regulations at 10 CFR Part 50, along with requirements that reactors establish procedures for responding to specific aircraft threat notifications.[20] Those regulations received final approval by the NRC Commissioners December 17, 2008.[21]

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-

[16] Nuclear Regulatory Commission, *Final Rule—Consideration of Aircraft Impacts for New Nuclear Power Reactors*, Rulemaking Issue Affirmation, SECY-08-0152, October 15, 2008.

[17] Nuclear Regulatory Commission, *Final Rule—Consideration of Aircraft Impacts for New Nuclear Power Reactors*, Commission Voting Record, SECY-08-0152, February 17, 2009.

[18] Nuclear Regulatory Commission, *Final Rule—Consideration of Aircraft Impacts for New Nuclear Power Reactors*, Rulemaking Issue Affirmation, SECY-08-0152, October 15, 2008, p. 2.

[19] Nuclear Regulatory Commission, "Power Reactor Security Requirments, Proposed Rule," 71 *Federal Register* 62664, October 26, 2006.

[20] Nuclear Regulatory Commission, "Power Reactor Security Requirements, Supplemental Proposed Rule," 73 *Federal Register* 19443, April 10, 2008.

[21] Nuclear Regulatory Commission, "NRC Approves Final Rule Expanding Security Requirements for Nuclear Power Plants," press release, December 17, 2008, http://www.nrc.gov/reading-rm/doc-collections/news/2008/08-227.html.

force" exercises, monitored by NRC, a mock adversary force from outside the plant attempts to penetrate the plant's vital area and simulate damage to 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.

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 Wackenhut, a security company that guards about half of U.S. nuclear plants, 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.[22] 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.[23] 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." NRC's 2007 annual security report to Congress found that the industry adversary teams "continued to meet expectations for a credible, well-trained, and consistent mock adversary force."[24]

The first three-year cycle of force-on-force exercises was completed for all 64 U.S. nuclear plant sites at the end of calendar year 2007.[25] During that period, 172 force-on-force exercises were conducted (an average of three per site), and 10 security inadequacies were cited. Two of the exercises, both in 2007, resulted in simulated damage or destruction of a vital target by the adversary team. If such an attack had been real, the plant could have released unacceptable levels of radioactivity. Both cases resulted from "the failure of licensee armed security personnel to interpose themselves between the mock adversary and the vital areas and target set components,"

---

[22] 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.

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

[24] Nuclear Regulatory Commission, Office of Nuclear Security and Incident Response, Report to Congress on the Security Inspection Program for Commercial Power Reactor and Category 1 Fuel Cycle Facilities: Results and Status Update; Annual Report for Calendar Year 2007, NUREG-1885, July 2008, p. 7, http://www.nrc.gov/reading-rm/doc-collections/congress-docs/correspondence/2008/boxer-07-01-2008.pdf.

[25] NRC generally lists 65 U.S. plant sites, but the adjacent Hope Creek and Salem sites in New Jersey are considered to be a single site for security exercises. E-mail message from David Decker, NRC Office of Congressional Affairs, March 13, 2009.

according to NRC's 2007 security report to Congress. In response to the failures, NRC imposed "immediate compensatory measures followed by long-term corrective actions." Follow-up force-on-force exercises were conducted to verify that the necessary security improvements had been made.[26]

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, proposals have been made to expand 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.

Spent Fuel Storage

When no longer capable of sustaining a nuclear chain reaction, highly radioactive "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 storage.[27] The

[26] Nuclear Regulatory Commission, Office of Nuclear Security and Incident Response, Report to Congress on the Security Inspection Program for Commercial Power Reactor and Category 1 Fuel Cycle Facilities: Results and Status Update; Annual Report for Calendar Year 2007, NUREG-1885, July 2008, p. 8, http://www.nrc.gov/reading-rm/doc-collections/congress-docs/correspondence/2008/boxer-07-01-2008.pdf.

[27] 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.

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.[28]

Long-term management of spent nuclear fuel is currently undergoing review, but spent fuel stored at reactor sites is expected to be moved eventually to central storage, permanent disposal, or reprocessing facilities. Large-scale transportation campaigns would increase public attention to NRC transportation security requirements and related security issues.

Security Personnel and Other Issues

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.[29] However, after a follow-up inspection into security issues at the Peach Bottom plant, run by Exelon Nuclear, 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."[30]

The incident drew harsh criticism from the House Committee on Energy and Commerce. "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, then-Chairman of the Committee.[31] NRC proposed a $65,000 fine on Exelon Nuclear on January 6, 2009.[32]

Following the 9/11 terrorist attacks, NRC conducted 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 orders to restrict security officer work hours,

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

[29] 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.

[30] Nuclear Regulatory Commission, *Security Officer Attentiveness*, NRC Bulletin 2007-1, Washington, DC, December 12, 2007.

[31] 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.

[32] Nuclear Regulatory Commission, "NRC Proposes $65,000 Fine for Violations Associated with Inattentive Security Guards at Peach Bottom Nuclear Plant," press release, January 6, 2009, http://www.nrc.gov/reading-rm/doc-collections/news/2009/09-001.i.html.

establish new security force training and qualification requirements, and increase the DBT that nuclear security forces must be able to defend against, as discussed previously.

In October 2006, NRC proposed to amend the security regulations and add new security requirements that would codify the series of orders issued after 9/11 and respond to requirements in the Energy Policy Act of 2005.[33] The new security regulations were approved by the NRC Commissioners on December 17, 2008, with the following provisions[34]:

- *Safety and Security Interface*. Explicit requirements are established for nuclear plants to ensure that necessary security measures do not compromise plant safety.
- *Mixed-Oxide Fuel*. Enhanced physical security requirements are established to prevent theft or diversion of plutonium-bearing mixed-oxide (MOX) fuel.
- *Cyber Security*. Nuclear plants must submit security plans to prevent cyber attacks on digital computer and communications systems and networks. The cyber security plan will become a license condition for each plant.
- *Aircraft Attack Mitigative Strategies and Response*. As discussed in the earlier section on vulnerability to aircraft crashes, nuclear plants must prepare strategies for responding to warnings of an aircraft attack and for mitigating the effects of large explosions and fires.
- *Plant Access Authorization*. Nuclear plants must implement more rigorous programs for authorizing access, including enhanced psychological assessments and behavioral observation.
- *Security Personnel Training and Qualification.* Modifications to security personnel requirements include additional physical fitness standards, increased minimum qualification scores for mandatory personnel tests, and requirements for on-the-job training.
- *Physical Security Enhancements*. New requirements are intended to ensure the availability of backup security command centers, uninterruptible power supplies to detection systems, enhanced video capability, and protection from waterborne vehicles.

A proposal by NRC staff to release more details about the results of nuclear plant security inspections was defeated by the NRC Commissioners in a 2-2 vote on January 21, 2009. Under current policy, NRC announces after a security inspection whether any violations that were found were of low safety significance or moderate-or-higher safety significance. Critics of the current policy contend that the public needs more detail to be assured of plant security. The policy's supporters counter that greater information about security inspection findings could inadvertently provide useful information to terrorists.[35]

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

[34] E-mail message from David Decker, NRC Office of Congressional Affairs, February 27, 2009.

[35] Jenny Weil, "Commissioners Reach Stalemeat on Security-Related Amendment," *Inside NRC*, February 2, 2009.

Author Contact Information

Mark Holt
Specialist in Energy Policy
mholt@crs.loc.gov, 7-1704

Anthony Andrews
Specialist in Energy and Energy Infrastructure Policy
aandrews@crs.loc.gov, 7-6843