Nuclear Power Plant Security and Vulnerabilities

Mark Holt
Specialist in Energy Policy

Anthony Andrews
Specialist in Energy and Defense Policy

August 28, 2012

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 issue following the attacks of September 11, 2001. Congress subsequently enacted new nuclear plant security requirements and has repeatedly focused attention on regulation and enforcement by the Nuclear Regulatory Commission (NRC). More than a decade after the 9/11 attacks, security at nuclear plants remains an important concern.

The Energy Policy Act of 2005 (EPACT05, 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, EPACT05 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 a "target set" of key safety components. From the start of the program through 2010, 136 force-on-force inspections were conducted, with each inspection typically including three mock attacks by the adversary force. During the 136 inspections, 10 mock attacks resulted in the simulated destruction of complete target sets, indicating inadequate protection against the DBT, and additional security measures were promptly implemented, according to NRC.

Nuclear power plant vulnerability to deliberate aircraft crashes has been a continuing issue. After much consideration, NRC published final rules on June 12, 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, deciding that other mitigation measures already required by NRC for all reactors were sufficient. 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. NRC published a broad final rule on nuclear reactor security March 27, 2009, including fire mitigation strategies and requirements that reactors establish procedures for responding to specific aircraft threats.

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 March 2009 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.

While NRC establishes security requirements within the boundaries of commercial nuclear sites, the Department of Homeland Security (DHS) has broad responsibility for coordinating government-wide efforts to prevent and respond to terrorist attacks, including attacks on nuclear power plants. DHS works with NRC and other agencies to protect nuclear facilities and other critical infrastructure.[1]

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. However, as the March 2011 Fukushima accident in Japan demonstrated, reactor containments cannot completely block radioactive releases under the most severe circumstances.

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.[2]

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 published regulations in June 2009 to require

[1] Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003, http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1.

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

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 a variety of additional nuclear plant security measures. In March 2009, NRC published a series of security regulations that require power plants to prepare cybersecurity 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 at specific nuclear plant sites through security plans, safeguards contingency plans, and guard training and qualification plans.

General requirements for the DBT are prescribed in NRC regulations,[3] 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."[4] 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.[5]

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

[3] 10 C.F.R. §73.1.

[4] 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.

[5] 10 C.F.R. §50.13. Attacks and destructive acts by enemies of the United States; and defense activities.

military organizations."[6] 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.[7]

In the Energy Policy Act of 2005 (EPACT05), Congress imposed a statutory requirement on the NRC to initiate rulemaking for revising the design basis threat.[8] EPACT05 required NRC to consider 12 factors in revising the DBT, such as an assessment of various terrorist threats, the potential use of substantial 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.[9] 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 the 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 as beyond the reasonable responsibility of a private security force, 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 NRC's final 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

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

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

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

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

airborne threats is addressed by other federal organizations, including the military."[10] Additional NRC action on aircraft threats is discussed in the next section.

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 vacant. In an interview afterward, NRC Chairman Dale Klein said the vote could be reconsidered after completion of an ongoing interagency study.[11] Critics contend that the DBT excludes major types of weapons used by terrorists, such as rocket-propelled grenades, and is generally not based on the maximum credible threat identified by the intelligence community.[12]

Critics of NRC's security regulations also have pointed out that licensees are required to employ only a minimum of 10 security personnel on duty per plant, which they argue is not enough for the job.[13] Nuclear spokespersons have 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). The industry also points out that nuclear plants all have integrated communications and emergency response plans that include local, state, and federal security forces. The integrated response by outside security forces is intended to handle attacks that might overwhelm an individual plant's security force.[14]

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.[15] 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. Fires and explosions caused by an aircraft crash outside the reactor containment could disable

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

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

[12] Edwin S. Lyman, "Security Since September 11th," *Nuclear Engineering International*, March 2010, pp. 14-19.

[13] 10 C.F.R. 73.55 (k)(5)(ii) states: "The number of armed responders shall not be less than ten (10)." The previous requirement, in 10 C.F.R. 73.55 (h)(3), stated: "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." The change was made in NRC final regulations published in March 2009, op. cit.

[14] Doug Walters, "Security Since March," *Nuclear Engineering International*, May 2010.

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

systems required to cool the reactor core and spent fuel pools, and post-9/11 NRC regulations require nuclear plants to be able to mitigate such effects. According to former NRC Chairman Nils Diaz, NRC studies, which have not been released, "confirm that the likelihood of both damaging the reactor core and releasing radioactivity that could affect public health and safety is low."[16] However, groups critical of nuclear power consider NRC's mitigation requirements for fires and explosions to be insufficient to protect against aircraft crashes.[17]

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. [18] 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 was drafted to 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 shield building with steel plates to increase resistance to aircraft penetration.[19]

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.[20] The NRC Commissioners, in a 3-1 vote, approved the change February 17, 2009, [21] and it was published in the Federal Register June 12, 2009.[22] The new rule added specific design requirements that all new reactors must meet:

> 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

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

[17] Committee to Bridge the Gap, Nuclear Information and Resource Service, and Public Citizen, "NRC Votes Against Requiring Reactors to be Protected from Air Attacks or Large Numbers of Attackers," press release, January 29, 2007, http://www.committeetobridgethegap.org/pressrelease/012907release.html.

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

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

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

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

[22] Nuclear Regulatory Commission, Consideration of Aircraft Impacts for New Nuclear Power Reactors, Final Rule, 74 *Federal Register* 28111, June 12, 2009. This provision is codified at 10 CFR 50.150.

(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. NRC determined that damage from aircraft crashes at existing reactors would be sufficiently mitigated by measures that had already been required by all reactors. 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.[23] 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).[24] 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.[25] Those regulations received final approval by the NRC Commissioners December 17, 2008,[26] and were published in the Federal Register March 27, 2009.[27] A key provision in the new rule states:

> Each licensee shall develop and implement guidance and strategies intended to maintain or restore core cooling, containment, and spent fuel pool cooling capabilities under the circumstances associated with loss of large areas of the plant due to explosions or fire, to include strategies in the following areas:
>
> (i) Fire fighting;
>
> (ii) Operations to mitigate fuel damage; and
>
> (iii) Actions to minimize radiological release.[28]

Spent Fuel Storage

When no longer capable of efficiently 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 many 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, or disable cooling systems so that cooling water evaporated, the spent fuel's zirconium cladding could overheat and catch fire.

---

[23] 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.

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

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

[26] 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.

[27] Nuclear Regulatory Commission, Power Reactor Security Requirements, Final Rule, 74 *Federal Register* 13925, March 27, 2009.

[28] 10 CFR 50.54(hh)(2).

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.[29]

NRC agreed with some of findings of the NAS study but disagreed in several areas. In a report to Congress in response to the NAS report, NRC stated:

> In summary, the NRC believes based on information developed in NRC vulnerability assessments, that the Committee has identified some scenarios that are unreasonable. The NRC also disagrees with some NAS recommendations and its conclusion lacks a sound technical basis. The NAS finding that earlier movement of spent fuel from pools into dry storage would be prudent is one such example.[30]

NRC conducted the site-specific analyses recommended by NAS with funding provided by the FY2006 Energy and Water Development Appropriations Act (P.L. 109-103, H.Rept. 109-275). NRC's March 2009 regulations cited above include "spent fuel pool cooling capabilities" as a function that must be addressed by nuclear plants' mitigation strategies for large fires and explosions. Protection of spent fuel cooling also is included in the design requirements for new reactors under NRC's June 2009 aircraft impact regulations.

NRC has long contended that the potential effects of terrorist attacks are not "reasonably foreseeable" impacts that must be included 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 outside the jurisdiction of the 9th Circuit.[31] The U.S. Court of Appeals for the 3rd Circuit subsequently ruled that NRC did not have to consider the impact of terrorist attacks in the license renewal application for the Oyster Creek plant in New Jersey.[32]

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. (For details, see CRS Report RL33461, *Civilian Nuclear Waste Disposal*, by Mark Holt.) Large-scale transportation campaigns would increase public attention to NRC transportation security requirements and related security issues.

---

[29] 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.

[30] U.S. Nuclear Regulatory Commission Report to Congress on the National Academy of Sciences Study on the Safety and Security of Commercial Spent Nuclear Fuel Storage, March 2005, p. iii, http://www.nrc.gov/reading-rm/doc-collections/congress-docs/correspondence/2005/domenici-03142005.pdf.

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

[32] U.S. Court of Appeals for the Third Circuit, *New Jersey Department of Environmental Protection v. U.S. Nuclear Regulatory Commission*, March 31, 2009, http://www.ca3.uscourts.gov/opinarch/072271p.pdf.

Force-on-Force Exercises

EPACT05 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, closely monitored and evaluated by NRC, a mock adversary force from outside the plant attempts to penetrate the plant's vital area and simulate damage to a "target set" of key safety components. Actual damage to such components could result in radioactive releases from the plant. 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, under NRC standards, a "composite adversary force" comprising security officers from many plants to simulate terrorist attacks in all force-on-force exercises conducted after October 2004. However, in September 2004 testimony, the Government Accountability Office (GAO) criticized the industry's selection of Wackenhut (now G4S Regulated Security Solutions), a security company that guards many U.S. nuclear plants, to manage the adversary force, including non-Wackenhut employees. 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.[33] 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.[34]

EPACT05 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 prohibits officers in the adversary force from participating in exercises at their home plants. As in previous years, NRC's 2010 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."[35]

---

[33] 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.

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

[35] 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 2010, NUREG-1885, Rev. 3, June 2011, p. 8, http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1885/r4/sr1885r4.pdf.

Through calendar year 2010, NRC had completed the second three-year cycle of force-on-force exercises at the 64 U.S. nuclear plant sites.[36] From the start of the program in 2004 through 2010, 136 force-on-force inspections were conducted, with each inspection typically including three mock attacks by the adversary force. During the 136 inspections, 10 complete target sets were simulated to be damaged or destroyed, indicating inadequate protection against the DBT, and additional security measures were promptly implemented, according to NRC. The inspections resulted in a total of 72 findings of security deficiencies, 58 of which were of relatively low significance. Follow-up force-on-force exercises are sometimes conducted to verify that the necessary security improvements have been made.[37]

Emergency Preparedness and 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 each plant to have an Emergency Planning Zone (EPZ) with an approximately 10-mile radius. Within the emergency EPZ, the plant operator must maintain warning sirens or other systems and regularly conduct emergency preparedness exercises evaluated by NRC and the Federal Emergency Management Agency (FEMA).

In light of heightened concern about terrorist attacks since 9/11, proposals have been made to expand the EPZ to include larger population centers. NRC determined that the 10-mile EPZ remained adequate, but it issued a bulletin in July 2005 identifying enhancements for emergency response plans in the case of "security-based events at a nuclear power plant."[38]

The potential 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.

NRC completed one of its final regulatory responses to the 9/11 attacks by issuing wide-ranging revisions to its emergency preparedness regulations on November 23, 2011. The changes include requirements that plant staff with emergency duties not have potentially interfering responsibilities; that hostile actions be included as a type of emergency that requires plant coordination with local, state, and federal agencies; that emergency plans include protection of plant personnel from hostile action; and that hostile actions be included in emergency preparedness drills. Some non-security changes were also included, such as a requirement that

[36] 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.

[37] NRC Office of Nuclear Security and Incident Response, *op. cit*.

[38] NRC Office of Nuclear Security and Incident Response, *Emergency Preparedness and Response Actions for Security-Based Events*, NRC Bulletin 2005-02, July 18, 2005, http://www.nrc.gov/reading-rm/doc-collections/gen-comm/bulletins/2005/bl200502.pdf.

evacuation time estimates be updated after every census or whenever major population changes occur.[39]

Cybersecurity

Existing U.S. nuclear power reactors, designed in the 1960s and '70s, are controlled primarily by analog systems that are resistant to cyberattack. However, new reactors are being designed with digital controls, and existing analog plants increasingly rely on computers to run auxiliary and monitoring systems. This increasing use of digital systems in nuclear power plants, along with post 9/11 security concerns and at least one "worm" infection at a U.S. reactor,[40] have prompted increased NRC attention to cybersecurity.

A year after the 9/11 attacks, NRC issued an order that included cyberattacks among the threats that nuclear plants would be required to defend against. Additional guidance for dealing with cyber threats was released during the next several years, and NRC issued formal cybersecurity regulations in March 2009 ("Protection of Digital Computer and Communications Systems and Networks," 10 CFR 73.54). NRC published a regulatory guide for the program in January 2010.[41]

NRC's cybersecurity regulations require each nuclear power plant to submit a cybersecurity plan and implementation schedule. The plan must provide "high assurance" that digital computer and communications systems that perform the following functions will provide adequate protection against design basis attacks:

- Functions that are safety-related or important to safety;
- Security functions;
- Emergency preparedness functions, including offsite communications; and
- Support systems and equipment that, if compromised, would adversely affect safety, security, or emergency preparedness functions.

Nuclear power plants are also required by the Federal Energy Regulatory Commission (FERC) to comply with cybersecurity standards issued by the North American Electric Reliability Corporation (NERC). However, nuclear plant computer systems that are covered by NRC security regulations are exempt from the NERC standards. As a result, the NERC standards apply mostly to "balance of plant" (non-reactor) systems at nuclear power plants.[42]

[39] NRC, "Enhancements to Emergency Preparedness Regulations," final rule, *Federal Register*, November 23, 2011, p. 72560.

[40] Kesler, Brent, "The Vulnerability of Nuclear Facilities to Cyber Attack," *Strategic Insights*, spring 2001, p. 15, http://www.nps.edu/Academics/Centers/CCC/Research-Publications/StrategicInsights/2011/Apr/SI-v10-i1_Kesler.pdf.

[41] NRC, "Cyber Security Programs for Nuclear Facilities," Regulatory Guide 5.71, January 2010, http://pbadupws.nrc.gov/docs/ML0903/ML090340159.pdf.

[42] Federal Energy Regulatory Commission, "Mandatory Reliability Standards for Critical Infrastructure Protection: Order Addressing Compliance Filing and Approving Implementation Plan," Docket No. RM06-22-011, March 18, 2010, http://www.nerc.com/files/CIP_ImplementationOrder-03182010.pdf.

Plant Security Personnel

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.[43] 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."[44]

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.[45] NRC proposed a $65,000 fine on Exelon Nuclear on January 6, 2009.[46] NRC modified its standards for plant security personnel in a major revision of its security regulations published March 27, 2009 (discussed in the next section).

Overview of NRC Actions after 9/11

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, 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.[47] The new security regulations were approved by the NRC Commissioners on December 17, 2008, and published March 27, 2009:[48]

- *Safety and Security Interface*. Explicit requirements were established for nuclear plants to ensure that necessary security measures do not compromise plant safety.

[43] 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.

[44] NRC, *Security Officer Attentiveness*, NRC Bulletin 2007-1, Washington, DC, December 12, 2007.

[45] 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.

[46] NRC, "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.

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

[48] *Federal Register*, March 27, 2009, op. cit.

- *Mixed-Oxide Fuel*. Enhanced physical security requirements were established to prevent theft or diversion of plutonium-bearing mixed-oxide (MOX) fuel.
- *Cybersecurity*. Nuclear plants must submit security plans that describe how digital computer and communications systems and safety-related networks are protected from cyberattacks, as discussed in the cybersecurity section above.
- *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.[49]

Author Contact Information

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

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

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