

DOCKET NUMBER
PROPOSED RULE PR 73
(70FR 67380)



**Union of
Concerned
Scientists**

Citizens and Scientists for Environmental Solutions

DOCKETED
USNRC

January 23, 2006 (2:25pm)

OFFICE OF SECRETARY
RULEMAKINGS AND
ADJUDICATIONS STAFF

January 23, 2006

Annette Vietti-Cook, Secretary
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

55

Submitted via e-mail to SECY@nrc.gov

ATTN: Rulemakings and Adjudications Staff

Dear Ms. Vietti-Cook:

Enclosed are comments on the proposed Design Basis Threat (DBT) rulemaking submitted on behalf of the Union of Concerned Scientists. Dr. Edwin Lyman and I collectively worked on these comments, which for the most part are extracted from our written testimony at open, public Congressional hearings on nuclear plant security since 9/11. Had the NRC not barred the public from the negotiations it held secretly with the Nuclear Energy Institute in crafting the proposed DBT rule, we would have gladly shared these points with the NRC earlier, too.

Sincerely,

David A. Lochbaum
Director, Nuclear Safety Project



Union of Concerned Scientists

Citizens and Scientists for Environmental Solutions

The Union of Concerned Scientists (UCS) submits its comments regarding the Nuclear Regulatory Commission's (NRC's) proposed rule entitled "Design Basis Threat." The proposed rule was published in the *Federal Register* on November 7, 2005, at 70 Fed. Reg. 67,380.

The NRC undertook this rulemaking effort to upgrade the design basis threat (DBT) in the aftermath of the 9/11 attacks. But no one should harbor any illusion that the DBT – in its proposed incarnation – can prevent tomorrow's attack for the very simple reason that it would not have prevented yesterday's attack. It is questionable public policy, at best, and regulatory malfeasance, at worst, for the NRC to take steps in response to a national tragedy that would be virtually useless in preventing a repeat of that tragedy.

Nuclear industry representatives and NRC officials often state that any attack on a nuclear power plant would not and could not harm people living and working outside its fences. Those statements mislead the public, undermine confidence in nuclear plant security preparedness, and are disrespectful to the thousands of Americans working long hours to prevent a successful attack. The truth is that a successful attack on a nuclear plant would be one of the worst disasters in American history. The utter fallacy of their statements is perhaps best revealed by two unassailable facts. First, the nuclear industry and the NRC urged Congress to renew Price-Anderson federal liability protection for nuclear power plants. If an attack could not cause harm outside nuclear plant fences, owners could get private insurance coverage and would not need Price-Anderson. Second, the nuclear industry claims to have spent more than \$1 billion upgrading nuclear plant security since 09/11. No one, particularly no one within the U.S. nuclear power industry, spends that kind of money on pseudo-hazards.

UCS has two basic concerns about security at U.S. nuclear facilities in the post-9/11 world that must be addressed in the NRC's DBT rule. First, some of these facilities possess highly-enriched uranium or plutonium, which can be used to make nuclear weapons, and this material is potentially vulnerable to theft by terrorists. Second, nuclear power plants remain too vulnerable to terrorist attacks that could result in the release of significant radiation – far more deadly than any "dirty bomb."

What we find most troubling is that we see little evidence of "outside-the-box" thinking going on in the NRC in response to emerging threats or safety concerns, reflected in the very minimal upgrades to the DBT in this rulemaking. The NRC does not want to question the assumptions they have made because they are afraid of the answers they might get, especially if those answers end up costing the industry more money. But the horrific events of 9/11 provide zero doubt that America's adversaries do not place similar constraints on themselves when plotting attacks. To match the intensity and commitment of the adversaries, the DBT rule must ensure that there is real, not surreal, protection of America's commercial nuclear facilities against both radiological sabotage and theft of weapon-usable materials. In the following sections, UCS details the changes to the DBT rule absolutely necessary to prevent the theft of weapon-usable materials and reduce the risk of successful sabotage at a nuclear power plant.

Theft of Weapon-Usable Materials

Only a relatively small number of NRC-licensed facilities possess significant quantities of highly enriched uranium or plutonium, which if stolen could be used to make nuclear explosive devices. These include a couple of fuel fabrication plants and a number of research reactors. But the NRC's responsibilities for regulation of the protection of nuclear materials against theft are growing in two key respects.

First, in the post-9/11 world there is greater concern about the potential for theft of weapon-usable fissile materials, in light of revelations that al Qaeda and other terrorist groups are intent on acquiring nuclear weapons. This calls into question, for example, the relatively lax security requirements that the NRC imposes on university research reactors that possess substantial quantities of highly enriched uranium.

Second, the number of NRC-licensed facilities that possess significant quantities of plutonium will increase if there is further action in the U.S. Department of Energy's troubled program to dispose of excess weapon-grade plutonium by converting it to mixed-oxide fuel (MOX) and irradiating it in commercial reactors. In April 2005, Duke Energy's Catawba plant in South Carolina became the first U.S. nuclear power plant in decades to qualify as a "Category I" plutonium facility by virtue of its receipt of 80 kilograms of plutonium contained in four MOX lead test assemblies — enough to make a dozen Nagasaki-type nuclear bombs. If the test is successful, at least one other site, Duke's McGuire plant in North Carolina, will take part in the program, and much larger quantities of plutonium-bearing MOX fuel will be shipped to both sites for years.

The NRC's approach to ensuring the security of materials at these facilities against theft should be evolving to keep pace with the growing threat, but it is not. Instead, the NRC is weakening the standards. This is a problem because, at the same time, the U.S. is trying to induce Russia to better protect its own weapon-usable material.

The DBT rule must provide real, substantive protection against theft of weapons-grade materials from U.S. nuclear facilities — power reactors, research reactors, and fuel cycle facilities.

Sabotage of Nuclear Power Plants

More than four years after the 9/11 attacks, UCS continues to have serious concerns about the adequacy of NRC efforts to reduce the vulnerability of nuclear power plants to radiological sabotage attacks. If a team of well-trained individuals were to succeed in gaining forced entry to a nuclear power plant, within a matter of minutes it could do enough irreversible damage to cause a meltdown of the core and a failure of the containment structure. Such an attack would have a devastating and long-lasting impact on public health, the environment, and the economy. A groundswell of public opposition to nuclear power would likely result, making it difficult for utilities to continue to operate existing nuclear plants, much less to construct new ones. The following section details ways in which the NRC must strengthen this DBT rule to better protect the public from the threats of sabotage of nuclear power plants.

The DBT describes the size of and other characteristics of the adversary group that certain nuclear facility licensees are required to design their security systems to protect against. There are different DBTs for the threat of radiological sabotage and for the threat of theft of "Category I" quantities of weapon-usable materials (2 kilograms or more of plutonium, 5 kilograms or more

of highly enriched uranium). On April 29, 2003, after a long deliberative process, the NRC issued revised DBTs to take into account the increased threat environment after the 9/11 attacks.

Nuclear power plant licensees and Nuclear Energy Institute (NEI) officials were allowed to review and comment on the proposed DBT orders, but members of the public were not. The NRC argues that the interests of the public were represented because it sought comment on the DBT from other agencies. In fact, most other agencies apparently did not endorse or support the NRC's proposed DBT. As NRC Commissioner Edward McGaffigan wrote in 2003:

*"...every other federal agency that reviewed the staff's proposed DBT, other than the FBI, felt there could be additional attributes in the DBT, but all of them declined to help us on where the line should be drawn between the primary responsibility of a regulated private sector guard force and the primary responsibility of government ... the agencies instead answered what the overall threat might be, and in my personal view covered their bets so that they could never be accused of underestimating terrorists ..."*¹

Ultimately, the NRC did not base the post-9/11 DBT on the maximum credible threat against U.S. critical infrastructure, as this comment suggests was the recommendation of most other agencies, but instead defined it as *"the largest reasonable threat against which a regulated private guard force should be expected to defend under existing law."* Although the DBT is "safeguards information" and is not publicly available, one can infer from public statements by NRC officials that it is not commensurate with the 9/11 attack threat — that is, a large group of attackers, capable of acting in four coordinated teams, that is assisted by several insiders and may have multiple large aircraft at its disposal.

This means that even today, more than three years after 9/11, private nuclear plant security forces would not be able to repel an attack on the magnitude of 9/11 on their own, but would require the assistance of additional forces (e.g. local law enforcement, National Guard) at public expense. Yet there is still no systematic mechanism in place to evaluate these vulnerabilities and quickly ensure that sufficient resources are provided to remedy them. Attempts to address these security gaps, like the Department of Homeland Security's National Infrastructure Protection Plan, which was issued in interim form in February of 2005, are a long way from being implemented.

While it is reasonable to exclude members of the public from deliberations regarding sensitive details of the DBT, public confidence is hard to sustain when the public knows that industry representatives are full partners at the table, and the table is behind closed doors. There should be some way to give taxpayers a say in deciding where to draw the line between private and public obligations, since they will be responsible for paying for the public resources needed to supplement the security of private nuclear facilities. Moreover, this taxpayer subsidy will only continue to increase if, as some industry representatives want, the DBT will remain frozen from now on, with the government paying to provide the additional security needed if the threat level increases in the future.

UCS persistently attempted to responsibly engage the NRC on security policy matters since 9/11. Recognizing that the NRC needed time to redraw the line between that information which could be openly discussed and that information which needed to be withheld but having security

¹ NRC Commissioner Edward McGaffigan, personal communication with UCS staffer Dr. Ed Lyman, May 16, 2003.

concerns that we felt the agency needed to understand as they made policy decisions, UCS and the Nuclear Control Institute (NCI) proposed that the NRC, on an interim basis, conduct meetings with the public on security issues similar to those held by their Advisory Committee on Reactor Safeguards (ACRS).² The ACRS holds public meetings where they hear presentations from NRC staff, industry representatives, and/or public interest group representatives. The information flow is largely one-way, from the presenters to the ACRS members. The presenters cannot question the ACRS members or otherwise extract information from them. The ACRS members have no obligation to express agreement or disagreement with the presenters during the public meetings. The ACRS members gather the information and consider it when forming their conclusions. UCS and NCI felt the NRC could use this meeting convention to listen to concerns from public stakeholders without undue concern about divulging safeguards/sensitive information. But the NRC denied our proposal.³

Understanding that the NRC's hands may very well be tied until it formally decides where the redrawn line is positioned and that UCS had the right to conduct our own meetings in the public arena, we invited the NRC to attend a meeting we would convene on nuclear plant security.⁴ We invited the NRC to participate in this meeting to the extent they were comfortable, but as a minimum we hoped they would attend and listen to the concerns expressed by UCS and other non-government organizations. But the NRC declined to attend in any capacity.⁵

The NRC refused our invitation *"because of the sensitive nature of the subject matter, we will consider meetings on security with appropriately cleared individuals on a case-by-case basis."* This rationale baffled us, because we know that NRC accepted several invitations to have their security personnel address meetings of the American Nuclear Society (ANS) and the Institute for Nuclear Power Operations (INPO).⁶ We know for certain that not every member of ANS attending these meetings had appropriate clearance. So, it appears that the NRC hid behind this screen only when it wanted to avoid meetings with groups like UCS. The NRC has clearly divided public stakeholders into two camps: those it will engage and those it will refuse to engage. We were not asking to be transferred to the other camp. We wanted the NRC to treat all public stakeholders fairly by only having one camp.

UCS last attempt to interface with the NRC on security was our proposal to have Mr. Paul Blanch represent UCS in security meetings with the NRC.⁷ Mr. Blanch obtained a safeguards clearance after 9/11 for work he was performing at the Indian Point nuclear plant in New York.

² Letter dated June 10, 2002, from Edwin S. Lyman, President, Nuclear Control Institute, and David Lochbaum, Nuclear Safety Engineer, Union of Concerned Scientists, to Chairman Richard A. Meserve, Commissioner Nils J. Diaz, Commissioner Greta J. Dicus, Commissioner Edward McGaffigan, Jr., and Commissioner Jeffrey S. Merrifield, Nuclear Regulatory Commission, "Request for Resumption of Public Meetings on Security." Provided as Attachment 4 to this statement.

³ Letter dated July 19, 2002, from Richard A. Meserve, Chairman, Nuclear Regulatory Commission, to David Lochbaum, Nuclear Safety Engineer, Union of Concerned Scientists. Provided as Attachment 5 to this statement.

⁴ Letter dated October 7, 2002, from Howard Ris, President, Union of Concerned Scientists, to Dr. Richard A. Meserve, Chairman, Nuclear Regulatory Commission. Provided as Attachment 6 to this statement.

⁵ Letter dated January 8, 2003, from Richard A. Meserve, Chairman, Nuclear Regulatory Commission, to Howard Ris, President, Union of Concerned Scientists. Provided as Attachment 7 to this statement.

⁶ Letter dated November 5, 2002, from Glenn M. Tracy, Director – Division of Nuclear Security, Nuclear Regulatory Commission, to David Lochbaum, Nuclear Safety Engineer, Union of Concerned Scientists. Provided as Attachment 8 to this statement.

⁷ Letter dated January 24, 2003, from David Lochbaum, Nuclear Safety Engineer, Union of Concerned Scientists, to Roy P. Zimmerman, Director – Office of Nuclear Security and Incident Response, Nuclear Regulatory Commission. Provided as Attachment 9 to this statement.

Mr. Blanch, familiar with our concerns about nuclear plant security, graciously agreed to represent UCS in NRC's closed-door security meetings. But the NRC denied this request.⁸ The NRC said that Mr. Blanch had a "need to know" while working at Indian Point, he lacked that "need to know" if working with UCS.

An examination of the numerous proposals UCS made to NRC clearly shows that UCS was not seeking equal access to information or equal time with NRC. We recognized and fully supported the need for NRC to meet behind closed doors with plant owners to discuss sensitive details of security requirements and their implementation. We merely sought an opportunity to articulate our security policy concerns to the NRC so the agency could give them due consideration when making policy decisions and developing this DBT rule. The NRC's continued rejection of our proposals and their inability to offer even a single counter-proposal since 09/11 sent us a strong message that the agency has no genuine interest in allowing public involvement in what very well may be the most important public policy issue of this new millennium.

That NRC's steadfast refusal to engage public stakeholders was just wrong was demonstrated all too clearly by the United States Congress. The Congress conducted numerous hearings on nuclear facility security after 9/11. Some of these hearings were closed to all but individuals with security clearances. But many of these hearings were open. UCS was invited to testify at several of these open, public Congressional hearings. These open, public hearings clearly showed that security policy matters could be responsibly conducted, even after 9/11. The NRC was clearly able to engage public stakeholders – it simply opted to deliberately avoid contact with the public it claims to protect while conspiring in secret with the industry it serves. This weak DBT rule was a product of that deliberate decision.

UCS believes the DBT must explicitly require protection against airborne attacks, both from large passenger jets and from small planes and helicopters potentially carrying explosives. NRC's current reliance on the protection against hijacking provided by Transportation Security Administration (TSA) procedures as the sole means of preventing an aircraft attack against a nuclear plant utterly fails to meet the NRC's fundamental goal of defense-in-depth. Since this rulemaking effort had its genesis in the 9/11 attacks, it is sadly ironic that it protects against another such attack largely by pretending it won't happen.

UCS also believes that the DBT must require better protection against land-based attacks. Land-based attacks can come from within the security fences, from outside the fences, and from a combination of inside and outside attacks. The NRC reduced the threat of insider sabotage by revising access authorization procedures after 09/11, but two additional low-cost measures must be addressed by the DBT rule. First, access to vital areas⁹ must be controlled better. The U.S. military applies the "two-person" rule for entry into areas containing key components of the atomic arsenal to make theft and tampering less likely. Likewise, the "two-person" rule for access to vital areas and/or expanded use of in-plant security monitoring cameras will lessen the likelihood of sabotage by insiders at nuclear plants. Many vital areas (e.g., the electrical switchgear rooms and the instrument rooms) are low-traffic areas that can be further protected by

⁸ Letter dated February 23, 2003, from Roy P. Zimmerman, Director – Office of Nuclear Security and Incident Response, Nuclear Regulatory Commission, to David Lochbaum, Nuclear Safety Engineer, Union of Concerned Scientists. Provided as Attachment 10 to this statement.

⁹ The NRC terms the land under and around a nuclear plant the owner-controlled area. The subset of that area demarked by the inner security fences is the protected area. The rooms within the plant containing equipment necessary to protect the nuclear fuel are vital areas. Most workers perform their assigned duties outside of the vital areas.

the “two-person” rule. Other vital areas (e.g., the control rooms) are high-traffic areas that are better protected by monitoring using in-plant cameras. These low cost measures¹⁰ would further reduce the likelihood of insider sabotage by better controlling access to areas containing vital equipment.

And UCS believes that the DBT must require better protection against waterborne attacks. Waterborne attacks seek to disconnect the nuclear plant from its adjacent lake, river, or ocean and prevent cooling of essential equipment and irradiated fuel. UCS commends the NRC for having undertaken some steps since 9/11 to better protect nuclear plants from waterborne attacks, but remains unconvinced that these steps are sufficient. The United States Navy reacted to 9/11 by installing floating barriers around ships at anchor in U.S. ports. For example, the Navy placed floating barriers, provided by Dunlop Industries of Scotland at a cost of \$10,000-15,000 per section, around its nuclear submarines at anchor in the Connecticut River in Groton as protection against its DBT. When the Department of Homeland Security conducted its assessment of vulnerabilities at the Millstone nuclear plant in Connecticut, the agency identified the cooling water intake structure as an unresolved vulnerability and offered to provide better protection against this threat, for free, to that plant’s owner. The owner declined this free upgrade and no protection has been added. This experience suggests to UCS that DHS was not persuaded that the steps mandated by NRC following 9/11 to upgrade protection against waterborne attacks was sufficient. The NRC’s DBT must require similar protective measures for the intake structures at nuclear power plants to provide Americans living in Connecticut and elsewhere with equal protection. If it’s right and prudent for the US Navy and recommended by DHS, it’s right and prudent and recommended for the US NRC.

Prior to 9/11, the NRC’s implementation of the DBT focused on ensuring the irradiated fuel in the reactor core was protected from damage by sabotage. That focus was incomplete. Many U.S. nuclear power plants have more than five times as much irradiated fuel in spent fuel pools and spent fuel dry casks as is in the reactor core. There are substantially fewer barriers that saboteurs must penetrate in order to successfully damage spent fuel and, correspondingly, there are fewer barriers protecting the public from radioactivity emanating from damaged spent fuel. It is essential, therefore, to also assure that spent fuel is adequately protected.

Today, spent fuel at U.S. nuclear power plants is woefully protected. Spent fuel pools are filled to overflowing with irradiated fuel. Spent fuel dry casks are stored out in the open in direct light-of-sight to areas easily accessible by the public and people contemplating harm. In fact, the current scheme of spent fuel storage maximizes the risk from both accidental and intentional damage to spent fuel and could hardly be made less safe or less secure. By maintaining the spent fuel pools at or near full capacity, the risk is kept as high as possible.¹¹ Transferring irradiated fuel assemblies into dry casks stored on open-air concrete pads merely adds risk to the maximized spent fuel pool risk.

The responsible thing to do would be to minimize the inventory of irradiated fuel in the spent fuel pools by transferring fuel discharged from the reactor more than five years ago into dry

¹⁰ UCS has not quantified the cost implications of these measures, but qualitatively compared them to practices currently in place at nuclear power plants. There are confined space entry requirements that a worker from entering a tank or other area alone or unmonitored where conditions may pose a health hazard. There are security cameras used to monitor exterior perimeters. The extension of these existing measures to better protect vital areas is relatively inexpensive.

¹¹ The risk factors are described on page 15 of U.S. General Accounting Office report GAO-03-426, “Spent Nuclear Fuel: Options Exist to Further Enhance Security,” July 2003.

casks emplaced within earthen berms or other protective devices. The risk reduction from emptying the spent fuel pool would more than offset the increased risk from dry cask storage, resulting in an overall tangible reduction in risk profile at the plant site. The DBT rule must explicitly address protection for spent fuel and must result in a lowered risk profile at U.S. facilities.

Force-on-Force Tests

A key aspect of a robust security program is force-on-force (FOF) testing up to the DBT level. The FOF testing program features a small group of mock intruders, called the adversary team, arrayed against the facility's armed guards. Security plans that look great on paper can have weaknesses that only become apparent during testing. UCS commends the NRC for instituting a mandatory FOF testing program, through its post-9/11 security orders, that will test the security of each plant site at least once every three years. The DBT rule must codify the testing frequency initiated by the orders. The credibility of this testing program is essential for public confidence. While the NRC has taken steps to make these tests more realistic, there are other issues that it must address to ensure the credibility of this program.

Having been deliberately excluded from the deliberative process that developed the DBT rule, the public must be able to trust the FOF tests. The public cannot have confidence in the outcomes of these tests unless their integrity is beyond reproach. But the NRC allowed NEI to award of the contract for the mock adversary team to be used in all FOF tests to Wackenhut, the same contractor that supplies the security officers for nearly half of US nuclear power plants. It is quite obviously extremely poor judgment and presents the potential for conflicts of interest. The FOF tests often pit Wackenhut attackers against Wackenhut defenders, turning the entire event into a farce-on-farce test of sanity. While NRC asserts that it is rigorously guarding against the possibility that the tests could be compromised, the public has no reason to take NRC at its word. After all, the NRC exercised unbelievably poor judgment in allowing the Wackenhut to test its own security readiness, leaving the public little reason to believe the agency's judgment will be any better in monitoring the FOF tests against "gaming."

In addition to being free from conflict of interest, the FOF tests must be challenging. The NRC must ensure that the attack scenarios chosen for the FOF tests are sufficiently challenging to provide high assurance that the licensees' security programs are robust. In particular, they should probe vulnerabilities in a licensee's protective strategy that are likely to be known by an insider in a top security position and could be exploited by real adversaries.

Also, FOF tests should not only test the ability of security forces to protect against the DBT, but should also evaluate the margin to failure of the security strategy with respect to increases in the threat beyond the DBT. Safety systems are typically designed with a margin to failure, so that they can continue to provide some protection even if design-basis accident conditions are exceeded. However, it is unclear if there is a comparable margin to failure with respect to security systems. The only way to determine this is to actually test the system with mock adversaries whose characteristics exceed the DBT in some respects.

Finally, the amount of time that licensees are given to prepare for FOF tests remains an issue. In a real attack, the element of surprise is one of the greatest advantages of the attacking force, but for practical reasons the NRC must give some advance warning of an impending test. This diminishes the usefulness of the test as an accurate measure of the state of security during day-to-day operations. Prior to 9/11, the NRC would inform licensees six to ten months in advance.

Recently, the Commission was informed in a public meeting that the NRC staff has reduced the period of advance warning to two months. However, this still allows far too much time for licensees to prepare for and rehearse for the test. For example, UCS learned from security personnel at some sites that the advance notice provides the opportunity for security guards to drill over and over from specifically designated posts. Thus, during the FOF test the security guards are well-practiced in their assignments responding to a simulated attack from those posts. But the reality of the situation is that security force personnel rotate assigned posts frequently during their shifts so there is no assurance that real attackers will assault a facility when guards are at their "trained" posts. FOF tests conducted with such long advance notice represent more theater than demonstration of security prowess.

The FOF tests must not unreasonably restrict the capabilities of insiders. The regulatory DBT specifies that the external adversary force is assisted by an insider that can participate in an active role, a passive role, or both. However, in the FOF tests conducted before 9/11, the role of the insider was limited to passive activities such as providing plant information to the external adversary team. But an active insider, who might be anyone from a control room operator to an armed responder, could give an enormous advantage to an adversary, and the serious threat such an insider could pose should not be ignored. Protective strategies should be developed with due consideration to the damage that could be caused by an active insider in any capacity, and those strategies should be fully tested in the FOF program.

The grading process for the FOF tests must be clear, understandable, and sensible. When NRC does a safety inspection and finds a problem, it uses a "significance determination process" (SDP) to evaluate the severity of the finding. For the most serious problems, such as those that have a high probability of leading to a core meltdown if left uncorrected, the process would generate a "RED" finding, which triggers a predetermined set of enforcement actions. For instance, for allowing the hole in the reactor vessel head to develop at Davis-Besse, First Energy clearly deserved, and got, a RED finding.

However, when the NRC tried to apply the same logic to evaluating the findings of FOF tests back in 2000, it ran into problems. For example, since the adversaries were considered to have achieved their goal in a FOF if they could have done enough damage to safety systems to cause a meltdown, the licensee would get a RED finding any time the adversaries "won" a FOF. Since the licensees were losing FOF drills about 50% of the time, they were not happy about this result. Consequently, the NRC suspended application of the process to FOF tests and went back to the drawing board.

Shortly before the 9/11 attacks, when this issue was still being discussed in public, the Nuclear Energy Institute made a proposal for an SDP process in which a FOF test could never result in a RED finding, no matter how badly a licensee's security force performed. The public never found out if the NRC adopted this proposal, since the 9/11 attacks intervened and the security SDP methodology was designated as "safeguards information." However, there was a public discussion of the SDP issue during a Commission briefing in March, and it appeared that the NRC is still experiencing problems with implementation of the security SDP, including disagreements with licensees over the results.

The public cannot have confidence in the FOF program if it does not have assurance that NRC is administering the most serious penalties when the most serious security violations occur.

Protection Above the DBT

The DBT defines the size and capability of potential attackers that nuclear power plant owners must protect against. The federal government provides protection against attacks above the DBT level per the “enemies of the state” provision.¹²

The key to protecting millions of Americans from radiological sabotage of nuclear power plants is not drawing the DBT line in the right place. The key is ensuring that there are no shortfalls in the protection provided by nuclear plant owners up to the DBT level and in the security measures taken by the federal government above it. When both sides of the DBT line are adequately secure, the actual placement of the line has negligible consequence on public health and safety. Conversely, when either side of the DBT line is inadequately secure, placement of the line at the absolutely correct spot fails to properly protect American lives. The NRC and the federal government should therefore ensure that both sides of the DBT line are adequately protected.

The FOF testing program discussed above can evaluate security readiness up to the DBT level, but it provides no measure of the protection against “enemies of the state” for which the federal government is responsible. The current emergency planning regulations for nuclear power plant disasters serve as the best model for how protection above the DBT level must be evaluated.

Adequate emergency planning requires the integrated efforts of the plant owner along with local and state authorities. Lines of communication must be established, training must be provided, and decision-making for application of resources must be clearly understood. By regulation, emergency planning is evaluated at each nuclear plant site at least once every two years in full participation exercises.¹³ The NRC assesses how well the plant owner meets his responsibilities. The Federal Emergency Management Agency (FEMA) assesses how well the local and state entities meet their responsibilities. FEMA is now part of the Department of Homeland Security (DHS).

The emergency planning concept should be used to evaluate protection against attacks larger than the DBT level. The actions taken by the federal government to protect the Wolf Creek nuclear plant in Kansas from enemies of the state are different than the actions taken to protect nuclear plants in Florida. The Coast Guard and Navy would not have a role to play at Wolf Creek as they would at nuclear plants situated on America’s shores. DHS should assess how well federal entities meet their responsibilities using periodic full participation exercises at all nuclear plant sites.¹⁴

Protection against enemies of the state has two components. When intelligence gathering and assessment identifies a credible pending threat against one or more nuclear plants, federal resources must be deployed to thwart the attack. When an attack precedes its warning, federal resources must be deployed in response. Periodic full participation exercises would allow DHS to assess the readiness of various federal entities in successfully discharging their protection and response functions.

¹² §50.13, “Attacks and destructive acts by enemies of the United States and defense activities,” of Title 10 of the Code of Federal Regulations, September 26, 1967.

¹³ 10 CFR 50, Appendix E and 44 CFR 350.9 paragraph (c)(1).

¹⁴ It may not be necessary to conduct an exercise for each nuclear plant site once every two years, as is currently done for emergency planning. When the same federal entities are involved in the protection for several nuclear plant sites, it may be adequate for Homeland Security to assess that grouping of entities in full participation exercises conducted at the individual sites on a rotating basis.

If the NRC assessed the capability of plant owners to defend against attacks up to the DBT level via challenging FOF tests every three years and DHS assessed the capability of the federal government to defend against larger attacks via periodic full participation exercises, the American people would have confidence that they were adequately protected from acts of malice at nuclear power plants whether the DBT level was too high, too low, or just right.

Specific Comments about the Proposed Rulemaking Language

These comments are based on the comparison between the old and new rules.

1. Replacement of terms “several persons” (radiological sabotage) and “small group” (theft of strategic special nuclear material) with “adversary team.”

UCS comment: This change will remove a limit on the potential size of the adversary team to a small number of individuals, and in principle could allow adversary teams on the scale of the September 11 attacks (19 individuals) or greater. However, the removal of any qualitative description of the adversary team size could, of course, also allow NRC to **reduce** the number of adversaries. Also, the public will never have an opportunity to discern whether the current number of adversaries in the radiological sabotage DBT, which by all accounts remains consistent with the description “several persons,” will ever increase to a level that UCS believes is consistent with the September 11 adversary force. For this reason, UCS believes that “adversary team” should be replaced with “large adversary team,” where the word “large” is understood in its conventional definition as “above average.” This will ensure that the level of protection mandated by the DBT rule will provide a safety margin against an “average” adversary team.

2. Increase in allowed number of independent teams and entry points for the radiological sabotage adversary.

UCS comment: The capability of an adversary team to attack in multiple independent teams at multiple entry points provides the adversary with a significant tactical advantage compared to an attack in a single team at a single entry point. For example, this allows for diversionary attack scenarios that would require more complex protective strategies to defeat.

The proposed rule change allows for a potential increase in the number of independent teams that the radiological sabotage adversary would be capable of operating as from one to more than one, and allows for the teams to attack at multiple entry points. If this option were consistently implemented, the radiological sabotage DBT would be enhanced.

However, the ambiguity in the proposed language does not **require** that licensees must protect against an adversary team attacking in more than one team at more than one entry point. The construction “one or more” is problematic. In the January 2005 hearing on the protection against theft of a Category I quantity of plutonium-bearing mixed-oxide fuel against at Duke Energy’s Catawba nuclear plant in South Carolina, Duke and the NRC staff advanced the theory that “two or more teams” actually meant that if the licensee could demonstrate protection against two teams, then it satisfied the rule and that

it didn't need to demonstrate protection against three teams, even if the number of adversaries were large enough to be split into three teams.¹⁵

In its decision on the case, the Atomic Safety and Licensing Board rejected the interpretation of the word "or" by Duke and the NRC staff and concluded that the rule required Duke to demonstrate protection against both "two teams" **and** more than two teams.¹⁶ However, the NRC Commissioners overturned the ASLB ruling in June 2005, and even though it did not comment specifically on this point, the rejection of the ruling leaves the phrase ambiguous once more. As a result, UCS requests that the construction "capable of operating as one or more teams" not be used. Instead, it should be replaced with "capable of operating in multiple teams, up to the maximum number of teams that can be formed from the adversary force, where a team has no fewer than two members." Similarly, "attacking from one or more entry points" should be replaced with "attacking from as many entry points as is possible with the allowed number of teams."

3. **Decrease in the allowed number of independent teams and entry points for the Category I theft adversary.**

UCS comment: In contrast to the proposed changes for the radiological sabotage adversary that would allow an increase in the number of teams and entry points, NRC is proposing to weaken the Category I theft adversary. In the current rule, the Category I theft adversary is already allowed to operate as "two or more teams," who presumably already have the capability to attack at multiple entry points. But in the proposed rule, this is changed to "one or more teams," which makes the Category I theft adversary identical to the radiological sabotage adversary. And taking into account the NRC staff interpretation of the construction "one or more" as discussed above, this would actually allow Category I theft licensees to satisfy the regulatory requirement by demonstrating protection against only one team attacking from a single entry point. This would be a weakening of the requirements for protection of Category I material (e.g. formula quantities of plutonium or highly enriched uranium).

In the current threat environment, UCS opposes any effort to **weaken** the security of nuclear-weapon-usable materials. Therefore, UCS requests, again, that the "one or more" be replaced with "up to the maximum number of teams that can be formed from the adversary force, where a team has no fewer than two members," and the same change as above to replace "one or more entry points."

4. **Near equivalence of radiological sabotage and Category I theft DBTs in proposed rule.**

UCS comment: The NRC's original intent in developing the DBT for theft of Category I material was that the theft threat should be more severe than the sabotage threat, since the potential consequences of a theft of weapon-usable material could be greater than the consequences of even the most severe radiological sabotage attack. This was reflected in part in the requirement in the current rule that the Category I adversary have the capability of operating as "two or more teams," whereas the radiological sabotage

¹⁵ Nuclear Regulatory Commission, Atomic Safety and Licensing Board, In the Matter of Duke Energy Corporation, Final Partial Initial Decision --- Public Redacted Version, LBP-05-10, April 18, 2005, p. 77.

¹⁶ Ibid, p. 84.

adversary did not have such a capability. In the proposed revision of the DBT rule, however, the two threats are rendered nearly identical.

UCS believes that the distinction between the threats of Category I theft and radiological sabotage should be maintained. UCS does agree that both the radiological sabotage DBT and the Category I theft DBT should be strengthened. Therefore, there should be a provision in the new rule to ensure that the Category I theft DBT always remains more severe than the radiological sabotage DBT. We would propose language to clarify that the adversary teams for theft and radiological sabotage are different, and that the Category I adversary team possesses greater capabilities with regard to number, training, equipment, weaponry and tactical skills than the radiological sabotage adversary.

5. Insider capabilities remain confusing.

UCS comment: The proposed rule for the insider capabilities retains the confusing construction “active ... or passive ... or both” that is in the current rule. UCS believes that protection must be provided against **both passive and active** insiders. The language should be replaced with “both active ... and passive ... insider assistance by knowledgeable individuals.”

6. Research reactors remain exempt from the DBT.

UCS comment: NRC has historically exempted research reactors from a requirement to protect against the design basis threats for both radiological sabotage and for theft, even for reactors that possessed Category I quantities of weapon-usable materials. This is a double-standard that is not appropriate. In light of the revelations of poor security at university research reactors on ABC News last fall, NRC must remove the exemptions for research reactors and require that they provide protection against design basis threats. For those reactors possessing Category I quantities of highly enriched uranium, they must provide theft protection at the same level as any other Category I facility. Research reactors that pose only a radiological sabotage threat should be required to protect against a DBT commensurate with the risk they could pose to public health and safety.

Comments prepared by:

David Lochbaum
Director, Nuclear Safety Project
Global Security Program
Union of Concerned Scientists

Dr. Edwin Lyman
Senior Staff Scientist
Global Security Program
Union of Concerned Scientists

From: "Dave Lochbaum" <dlochbaum@ucsusa.org>
To: <SECY@nrc.gov>
Date: Mon, Jan 23, 2006 1:27 PM
Subject: UCS comments on NRC's Design Basis Threat (DBT) rulemaking

Good Day:

Attached please find comments submitted on behalf of the Union of Concerned Scientists about the NRC's proposed DBT rulemaking. The November 7, 2005, Federal Register notice indicated that comments could be submitted electronically. UCS selected this option and will not be also sending in a hard copy of the attached comments. If there is any problem opening the attachment or understanding its contents, please contact me.

Thanks,

Dave Lochbaum
Director, Nuclear Safety Project
Union of Concerned Scientists
1707 H Street NW Suite 600
Washington, DC 20006-3962
(202) 223-6133 (office)
(202) 331-5430 (direct line)
(202) 223-6162 (fax)

CC: "Glenn Tracy" <GMT@nrc.gov>

Mail Envelope Properties (43D51FF6.4A4 : 9 : 42148)

Subject: UCS comments on NRC's Design Basis Threat (DBT) rulemaking
Creation Date: Mon, Jan 23, 2006 1:27 PM
From: "Dave Lochbaum" <dlochbaum@ucsusa.org>

Created By: dlochbaum@ucsusa.org

Recipients

nrc.gov
 TWGWPO02.HQGWDO01
 GMT CC (Glenn Tracy)

nrc.gov
 owf5_po.OWFN_DO
 SECY (SECY)

Post Office
 TWGWPO02.HQGWDO01
 owf5_po.OWFN_DO

Route
 nrc.gov
 nrc.gov

Files	Size	Date & Time
MESSAGE	655	Monday, January 23, 2006 1:27 PM
TEXT.htm	1203	
20060123-ucs-nrc-dbt-rulemaking-comments.pdf	422911	
Mime.822	582232	

Options

Expiration Date: None
Priority: Standard
Reply Requested: No
Return Notification: None

Concealed Subject: No
Security: Standard