

**DOCKET NUMBER**  
**PROPOSED RULE PR 73**  
**(70FR 67380)**

99

**NUCLEAR INFORMATION AND RESOURCE SERVICE**

1424 16<sup>th</sup> Street NW Suite 404

Washington, DC 20036

Tel. 202 328 0002

[www.nirs.org](http://www.nirs.org)

DOCKETED  
USNRC

February 22, 2006

February 23, 2006 (3:29pm)

Office of the Secretary  
United States Nuclear Regulatory Commission  
Washington, DC 20036  
Attention: Rulemaking and Adjudications Staff

OFFICE OF SECRETARY  
RULEMAKINGS AND  
ADJUDICATIONS STAFF

By Email: [SECY@nrc.gov](mailto:SECY@nrc.gov)

**Comments of Nuclear Information and Resource Service (NIRS) on Proposed  
Rulemaking to Modify the Design Basis Threat for Nuclear Facilities and Request  
that the Agency Withdraw RIN-3150-AH60**

To whom it may concern:

Attached please find the comments of Nuclear Information and Resource Service (NIRS) pertaining to the November 7, 2005 Notice of Proposed Rulemaking as originally posted in the Federal Register, November 7, 2005 (Volume 70, Number 214, Page 67380-67388) to amend the Design Basis Threat regulations for nuclear power plants and nuclear materials facilities.

NIRS is concerned that the proposed rule as written reflects the Commission's misguided efforts to contain the real cost of security at US nuclear power stations. The present joint Commission and industry plan to codify the Design Basis Threat is made at potentially great expense to the public health, safety and security by maintaining an unrealistically low level security bar around nuclear power stations which has already been surpassed by the tragically consequential al-Qaeda attacks on domestic soil.

We urge that the Commission withdraw the proposed rule (RIN-3150-AH60) as written, re-evaluate and complete an analysis of the twelve factors as published in the Federal Register notice incorporating the lessons learned from and since the September 11<sup>th</sup> attacks and reissue an appropriately upgraded DBT rule for public comment.

Sincerely,

Paul Gunter, Director  
Reactor Watchdog Project

ATTACHMENT: NIRS comments

## **Background**

The Design Basis Threat or "DBT" is defined as the magnitude of threat that each nuclear facility's security systems must be capable of defending against with a high level of confidence. Originally crafted by NRC in the 1970's, the DBT now remains practically unchanged for more than 30 years. The DBT defines the composition and characteristics of an adversary force including their degree of military training, the weapons they are expected to carry, their mode of attack and level of knowledge of target sets and site defensive vulnerabilities. Prior to September 11th 2001, nuclear power station security forces were tested by NRC contractors in "Force-On-Force" mock terrorist attacks or Operational Safeguard Response Evaluations (OSRE) once every 8 years. The security exams, pre-announced to utilities 6 months ahead of time and role played with licensees in table top exercises in advance of actual mock attack, limited the "attacking" force as defined by the DBT to a single team of three military-experienced contractors attacking on foot by land assisted by one passive insider. Even so, the mock attackers penetrated defenses and simulated sabotage of onsite equipment 47% of the time so as to cause a simulated core melt accident, often in a matter of seconds to a few minutes. In 1998, at the behest of industry, NRC management zeroed out the budget for the OSRE program only for it to later be restored through media exposure by an agency whistleblower and the actions by President Bill Clinton. However, the nuclear industry continued to stonewall security upgrades as unnecessarily sophisticated and overly expensive, culminating in a draft NRC policy to turn over security testing to an industry self-assessment program to begin its pilot phase in September 2001.

Following the September 11th attacks, the industry abandoned its pilot self assessment program and NRC suspended all site security testing as well as public stakeholder meetings to reevaluate nuclear power's protective strategies and NRC security policy. After conferring with industry while excluding public stakeholders, NRC issued secret "Orders" on April 29, 2003 purportedly altering the DBT, including a change to now conduct OSREs every three years, for industry compliance by October 29, 2004. While the DBT is "classified" NRC concedes that it still does not require licensees to protect against the numbers of attackers or their level of coordination as experienced on September 11<sup>th</sup> (a minimum of 19 attackers coordinated into four teams), nor against air attack. Given the disclosure of the controversial history of cost-driven nuclear security, there is no public confidence in a secretly revised DBT that does not match the level of sophistication and ferocity already demonstrated by the attacks on the World Trade Center and Pentagon nor does its secrecy provide enough substance for the public to meaningfully comment on.

Despite this lack of public confidence, NRC now seeks to codify those Orders through the current proposed rulemaking derived in large part as a cost benefit analysis.

However, the validation of the questionable adequacy of the April 29, 2003 security orders as the established required security levels as well as the equally questionable rigor of federal oversight as would be codified by this proposed rulemaking remain of dire concern. On September 14, 2004, House Subcommittee on National Security, Emerging

Threats and International Relations, chaired by Rep. Chris Shays (R-CT), held a hearing to receive Government Accountability Office (GAO) testimony on compliance with the Oct. 2004 deadline [ <http://www.gao.gov/new.items/d041064t.pdf> ]. It concluded that the rush to review facility plans for implementing the new DBT orders "is largely a paper review." NRC did not visit sites to verify compliance nor request facilities to submit documents that supported security upgrades. In fact, GAO concluded it will be years before NRC will have data to validate whether site-specific upgraded security plans are adequate. Congressman Shays concluded: "Despite persistent efforts by reactor operators and regulators to minimize the risks of containment breach or spent fuel sabotage, surrounding communities and those farther downwind take little comfort from a cozy, indulgent regulatory process that looks and acts very much like business as usual."

**The "Cozy Relationship" between NRC and the Nuclear Industry as Expressed by the Proposed Rulemaking Significantly Undermines Public Health, Safety and Security by Codifying an Unreasonably Low Security Bar Around Nuclear Facilities as Part of an NRC Supported Industry Cost Analysis**

Prior to the 9/11 attacks, NIRS participated in a number of NRC and industry public meetings regarding "business as usual" security levels at nuclear power stations. It was our direct observation that the industry consistently argued that it was unreasonably being required to expend its financial resources on unrealistic adversary characteristics and overly sophisticated threat levels. As such, the security bar around nuclear power stations was maintained unreasonably low given what we now know as documented by the National Commission on Terrorist Attacks on the United States publicly released on July 22, 2004 [ <http://www.9-11commission.gov> ]. "The 9/11 Commission Report" as it is called cites that al-Qaeda had originally contemplated hijacking 10 commercial airliners and flying two of them into US nuclear powers along with the World Trade Center, the Pentagon, the Capitol and other targets.<sup>1</sup>

Site defenses against a ground attack were unrealistically limited to small single unit force acting with a single passive insider. Airborne and water borne attacks were not considered. As described in Time Magazine,

*"Before 9/11, the agency required plants to be able to thwart an attack by little more than an armed gang---three outsiders equipped with handheld automatic weapons and aided by a confederate working inside the plant. After 9/11 when al-Qaeda showed the ability to produce 19 operatives for a suicide mission on a single day, some security specialists anticipated a significant hike in the DBT. But the number of attackers in the revised DBT is less than double the old figure and a fraction of the size of the 9/11 group."*<sup>2</sup>

---

<sup>1</sup> "The 9/11 Commission Report," The National Commission on Terrorist Attacks Upon the United States, July 22, 2004, page 154.

<sup>2</sup> "Are These Towers Safe: Why America's Nuclear Power Plants are Still So Vulnerable to Terrorist Attack-and How to Make Them Safer. A Special Investigation," TIME, Mark Thompson, June 20, 2005.

Repeated public interest efforts to upgrade the DBT have by and large failed to significantly move the NRC and the industry to take appropriate protective actions, most recently including the post-9/11 Proposed Rulemaking 73-12 as filed by Committee to Bridge the Gap (CBG). Despite more than 800 comments, overwhelming in favor of increasing the DBT to defend against a 9/11 equivalent adversary force as well as aircraft attack, the Nuclear Regulatory Commission and the nuclear industry continue to perpetrate the increasingly dangerous myth that a nuclear power station can not be successfully attacked by aircraft (hijacked, contracted or private). Of further concern, despite the devastating evidence of September 11, 2001 attacks, NRC and the industry fail to prepare for an adversarial force of its equivalent comprised of at minimum nineteen attackers coordinated into four teams willing to die in order to strategically inflict massive casualties and widespread economic dislocation.

The modest efforts put in place by the 2003 Orders have failed to adequately raise the defense bar around nuclear power and research reactors but instead raise substantive concerns about the inadequate level of security being maintained by the nuclear industry and the rigor of federal policy and regulatory oversight.

For example, even without the public obtaining security clearance for classified safeguards information, we plainly observe that there are no marine intrusion prevention devices protecting the cooling water intake systems for most U.S. nuclear power stations. Without such protection, once-through cooling intake systems are vulnerable to high-level explosive attack borne by boat, barge, submarine or suicidal SCUBA teams.

Additionally, the fact remains that there are no aircraft attack defense systems or structures around a broad range of potentially vulnerable nuclear power station target sets. Moreover, the absence and artificiality of the air attack security is in example by the NRC Emergency Action Levels (EAL). The aircraft threat actuation levels for the onsite emergency operations center and as such preparedness for the initiation of offsite emergency plans for protective actions completely discount a wide range of potential adversarial aircraft, including easily commandeered private aircraft that if laden with high explosives and shaped charges could strike unannounced into highly radioactive targets such as those publicly identified in the April 2005 National Academy of Sciences Report "Safety and Security of Commercial Spent Nuclear Fuel Storage Systems."<sup>3</sup>

As TIME magazine reported, NRC documents indicate that nuclear power stations do not maintain adequate security forces to repel a September 11<sup>th</sup> size adversarial force (a minimum of 19 attackers in four coordinated teams) with a high degree of confidence.

More disturbing is the fact that this artificially low and antiquated security standard as proposed to be codified is conceived and maintained by NRC and industry as a cost containment strategy to protect the financial interest of the nuclear industry. The prioritization of security cost over national security was acknowledged as a public health and safety concern by one of NRC's own security specialists. This is first documented in the Differing Professional Opinion of Captain David Orrik who directed the

---

<sup>3</sup> The National Academy of Sciences Report on "Safety and Security of Commercial Spent Nuclear Fuel," April 06, 2005

aforementioned Operational Safeguard Response Evaluations. In Captain Orrik professional opinion and objections, he identifies that the mock force-on-force evaluations at nuclear power stations resulted in mock adversaries successfully reaching on-site target sets at 47% of the U.S. reactors evaluated.<sup>4</sup> What NRC staff subsequently described as “some minor weaknesses” at these sites was identified by the DPO as “In fact, all of the weaknesses, not ‘some,’ related to a demonstrated inability to prevent mock adversary forces from gaining access to vital equipment which could, if sabotaged, cause core damage and radioactive release. For example, 14 of these plants were unable to prevent mock adversary forces from gaining (simulated) access to containment.”<sup>5</sup> The DPO documented “nothing less than the abject failure by the nuclear industry to be capable---by themselves---of protecting against radiological sabotage.”<sup>6</sup> The professional opinion and objection further stated that “there is increasing pressure throughout the nuclear power industry to reduce costs, and security forces are taking direct hits; reduction in annual budgets, reductions in numbers of security officers. A countervailing pressure is necessary.”<sup>7</sup>

Such “countervailing pressure” was demonstrated on September 11, 2001 just as the Nuclear Energy Institute was to begin its NRC-approved pilot industry self-assessment security program, “Security Performance Analysis” to replace the troublesome and increasingly expensive Operational Safeguard Response Exercises.

While NEI and a bowed Nuclear Regulatory Commission were busy reducing oversight and seeking to contain security costs for nuclear power stations, the al Qaeda attacks were scaled back to the four hijacked aircraft.

Even more disturbing is the fact that this joint government/industry-led cost containment strategy was achieved and is further maintained through a policy of close door meetings that bar the reasonable requests for the public’s right-to-know and the protection of democratic interests under a post 9/11 guise of protecting safeguards information in the interest of public health, safety and security. To the contrary, this joint secret rulemaking effort as conceived to in fact protect the financial interests of the nuclear industry further jeopardizes national security by now proposing to codify an artificially low security bar around nuclear power stations as a means of providing financial security a competitively beleaguered nuclear power industry.

### **The Proposed Rulemaking Fails to Comply with the Administrative Procedures Act**

The Administrative Procedures Act (APA) requires proposed rules to be issued for public review and comment before being adopted as final rules. Instead, NRC has issued the proposed DBT changes in such a form as to reveal nothing of substantive content of the

---

<sup>4</sup> “Differing Professional Opinion Regarding NRC’s Reduction of Effectiveness and Efficiency in the ‘Staff Recommendations’ of the Follow-on OSRE Program for Nuclear Power Plants,” Captain David Orrik,(ret), U.S. NRC, Security Specialist, Office of Nuclear Reactor Regulation, United States Nuclear Regulatory Commission, February 3, 1999.

<sup>5</sup> Ibid, page 3.

<sup>6</sup> Ibid, page 4.

<sup>7</sup> Ibid, page 4.

proposed changes amounting to secret Orders applicable to its regulated nuclear licensees. NRC now seeks to codify these secret changes further avoiding public scrutiny on matters affecting their health, safety and security.

Public Citizen and The San Luis Obispo Mothers for Peace have challenged the NRC in federal court contending that the agency illegally issued new orders without providing an opportunity for public participation promulgating new regulations that that secretly changed security standards and requirement for nuclear facilities.

These petitioners have argued that the Administrative Procedure Act and the Atomic Energy Act required NRC to submit DBT changes through an open rulemaking process in which the public would have an opportunity to participate and comment. Because NRC's DBT order specifically noted that it superseded the long-established DBT regulations in 10 C.F.R. § 73.1, the petitioners argued, and because it creates policies applicable prospectively across the board, it must be considered a regulation. The NRC and industry's closed rulemaking process and the secret details of the rule make the entire DBT change an impermissible secret rulemaking which NIRS further charges has unreasonably prioritized an industry cost containment strategy throughout its clandestine process.

### **The Proposed Rule Fails to Comply with the Intent of Congressional as Assigned by the Energy Policy Act**

Congress directed NRC in the Energy Policy Act of 2005 to undertake the upgrading of the DBT by rulemaking and in so doing considering 12 factors including an analysis of the September 11<sup>th</sup> attacks using aircraft coordinated into four separate attacks involving at minimum 19 adversaries.

Instead, NRC's proposed rulemaking asks the public to comment "on whether or how the 12 factors should be addressed in the DBT rule."

In our view, this is a deliberate dodge of NRC's obligation to directly answer to Congressional concerns on the perceived inadequacy of the DBT and as such national security stemming for under protected radiological targets.

### **Conclusion**

NIRS urges the NRC to withdraw this ill conceived proposed rulemaking to amend the DBT as fashioned to protect the nuclear industry's financial bottom line at the expense of inadequate public health, safety and security potentially affected by successful terrorist attacks on these radiological targets.

NRC needs reissue a proposed DBT with adequate enough detail so that the public can discern that it is commenting on whether or not nuclear site defensive forces need to be raised to numbers and training adequate enough to confidently protect against the equivalent of a September 11<sup>th</sup> adversarial force or whether vulnerable irradiated nuclear

fuel storage ponds should remain vulnerable to attack by commandeered explosive laden aircraft, or whether cooling water intake systems should continue to remain vulnerable to coordinated land attacks and/or by explosive laden boats, barges or submarines. These are some of the decisions that NRC and the nuclear industry have instead made in secret while considering how best to first protect the industry's financial interests over adequately protecting the public health, safety and security.

Sincerely,

Paul Gunter, Director  
Nuclear Information and Resource Service  
1424 16<sup>th</sup> Street NW Suite 404  
Washington, DC 20036  
Tel. 202 328 0002  
[www.nirs.org](http://www.nirs.org)  
Email: [pgunter@nirs.org](mailto:pgunter@nirs.org)

**From:** "Paul Gunter" <pgunter@nirs.org>  
**To:** <SECY@nrc.gov>  
**Date:** Wed, Feb 22, 2006 7:35 PM  
**Subject:** NIRS comments RIN-3150-AH60

Hello,

Attached please find the comments of Nuclear Information and Resource Service (NIRS) comments and request that NRC withdraw RIN-3150-AH60.

Sincerely,

Paul Gunter, Director

Reactor Watchdog Project

Nuclear Information and Resource Service

1424 16th Street NW Suite 404

Washington, DC 20036

Tel. 202 323 0002

[www.nirs.org](http://www.nirs.org) <<http://www.nirs.org/>>



**Mail Envelope Properties** (43FD0329.6D9 : 15 : 42713)

**Subject:** NIRS comments RIN-3150-AH60  
**Creation Date:** Wed, Feb 22, 2006 7:35 PM  
**From:** "Paul Gunter" <[pgunter@nirs.org](mailto:pgunter@nirs.org)>

**Created By:** [pgunter@nirs.org](mailto:pgunter@nirs.org)

**Recipients**

nrc.gov  
owf5\_po.OWFN\_DO  
SECY (SECY)

**Post Office**

owf5\_po.OWFN\_DO

**Route**

nrc.gov

**Files****Size****Date & Time**

MESSAGE

374

Wednesday, February 22, 2006 7:35 PM

TEXT.htm

2977

security02222006dbtpmnrscmts.doc

60416

Mime.822

88162

**Options**

**Expiration Date:**

None

**Priority:**

Standard

**Reply Requested:**

No

**Return Notification:**

None

**Concealed Subject:**

No

**Security:**

Standard