

DOCKET NUMBER
PROPOSED RULE PR 73
(70FR 67380)

From: Michel Lee <ciecplee@optonline.net>
To: <SECY@nrc.gov>
Date: Mon, Jan 23, 2006 4:08 PM
Subject: NRC Proposed Rulemaking (RIN 3150-AH60) - SUBMISSION OF COMMENTS ON UPGRADING OF DBT

57

Re: NRC Proposed Rulemaking (RIN 3150-AH60)

DOCKETED
USNRC

This Transmission Constitutes a Submission of Comments to NRC on Upgrading of DBT

January 24, 2006 (11:15am)

OFFICE OF SECRETARY
RULEMAKINGS AND
ADJUDICATIONS STAFF

Nearly five years after September 11, 2001, the 103 civilian nuclear reactors in the United States are still not in a position to repel attacks by adversaries with capabilities commensurate with those of either the 9/11 terrorists or with enemies of the United States currently operative on the world stage. The present Design Basis Threat (DBT) thus falls far short of the actual threat level faced by the U.S. today, much less the escalated level the nation will face as nations such as Iran and North Korea improve and export nuclear engineering expertise. Indeed, as numerous security experts have pointed out, a terrorist group with access to sympathetic nuclear scientists and engineers would have sufficient sophistication to target the critical systems and weak links of nuclear reactors. The assistance that Pakistani nuclear scientists reportedly offered to Al Qaeda illustrates this threat.

Al Qaeda and other terrorist groups have shown extraordinary tactical ingenuity and a complete lack of reverence for human life. The increasing military sophistication displayed by insurgents and terrorists during the current operation in Iraq also demonstrates that a sizable, well-planned and orchestrated military operation against a nuclear facility is well within current terrorist capability.

Consequently, the COUNCIL ON INTELLIGENT ENERGY & CONSERVATION POLICY (CIECP) urges the NRC to address the following realities:

ACTIVE INSIDERS

The voluminous number of security breaches which have occurred at critical infrastructure, including nuclear weapons and power facilities after 9/11 (such as the 16 foreign-born construction workers who were able to gain access to the Y-12 nuclear weapons plant with falsified

Template = SECY-067

SECY-02

documentation) demonstrates that nuclear "insiders" must be deemed potential active participants in an attack. The increasing reliance of nuclear power plant operators upon outsourcing of on-nuclear site work to independent contractors in order to cut costs further augments this threat. Such participation need not occur during the engagement, it might occur days or even many months prior to an attack and involve actions such as surveillance of plant schematics, security features and protocols. Pre-attack participation could also involve the sabotage of critical instrumentation, computers, electronic systems or any number of other components, where such sabotage would likely not be discovered prior to an emergency event.

COMPUTER SYSTEM COMPROMISE

Nuclear power plant computer systems, like those of other critical infrastructure, are subject to a range of vulnerabilities, including power outages, attacks by malicious hackers, automated softwares, viruses and worms. Many terrorist networks have the resources and technical savvy to wreak havoc. (For example, the alleged terrorist, Muhammad Naeem Noor Khan, picked up in Pakistan in 2004, and believed to have links with Al Qaeda, is a computer engineer.) The fact that U.S. nuclear reactors are not impregnable was demonstrated by the penetration of the Slammer worm into the Davis-Besse nuclear reactor. That intrusion disabled a safety monitoring system for nearly 5 hours. The vulnerability of nuclear computers to acts such as the sabotage of off-site power transmission was evidenced at the Indian Point nuclear power plant during the 2003 blackout which struck the Northeast. At Indian Point, various computer systems had to be removed from service, including the Critical Function Monitoring System, the Local Area Network, the Safety Assessment System/Emergency Data Display System, the Digital Radiation Monitoring System and the Safety Assessment System. It is, accordingly, a matter of pressing importance that the NRC engage independent experts to develop a comprehensive computer vulnerability and cyber-attack threat assessment. Such an assessment must evaluate the vulnerability of the full range of nuclear power plant computer systems and the potential consequences of such vulnerabilities. The revised DBT must incorporate such findings and include a protocol for quickly detecting such an attack and recovering key computer functions in the event of an attack.

CHEMICAL WEAPONS

The DBT must address the possibility that toxic chemicals could be part of an attack scenario. There are numerous agents that can be deployed with almost instantaneous effect and can immobilize targets via paralysis, convulsions, blinding, suffocation or death. Such agents could be employed as part of the initialization strategy. For, example, a truck or even large SUV filled with chlorine, boron trifluoride,

hydrofluoric acid, liquid ammonia, or any number of other agents could be crashed into a perimeter barrier, with the resulting fumes killing or disabling plant personnel guarding the outdoor area of the facility. Chemical agents could also be introduced surreptitiously into building ventilation systems. They could also be used strategically to neutralize workers endeavoring to maintain control of the situation. Many such chemical agents are easy to make and do not require sophisticated delivery systems. Some can be carried in coffee mugs or in vials within body cavities. Phenarsazine chloride, an arsenic derivative, can be transported in minute quantities, even as a powder that can be dusted on paper. It is lethal if burned and even a spoonful can cause immediate extreme irritation of the eyes and breathing passages. A chemical like chloroform acetone methanol can be transported on filter paper, then combined with a heat source to create an explosion.

PLANTS MUST BE ABLE TO MOUNT A FULL DEFENSE WITHOUT RELIANCE ON OUTSIDE ASSISTANCE

Numerous studies and the actual events of 9/11, Katrina, and Rita (as well as relatively minor events such as the January 18, 2006 wind storm in NY) demonstrate beyond cavil that first responder forces and the National Guard do not have the resources, manpower, equipment or communications capabilities to swiftly and adequately respond to a major assault on a nuclear facility. In some regions - most notably the New York Metropolitan region, in which the Indian Point nuclear power plant is sited - roadway logistics and regular congestion alone would likely prevent assisting forces from reaching a nuclear plant under attack in time. (Notably, SWAT team assembly takes approximately 2 hours, an assault could be over in a matter of minutes.) It is accordingly crucial that the NRC eliminates the faulty assumption, contained in the current DBT, that plant personnel need only fight off attackers until law enforcement or military aid arrives. The fact that most regional first responders have little detailed knowledge of either the operational or internal layout of nuclear facilities further testifies to the folly of reliance upon the "cavalry".

A COORDINATED ATTACK ON MULTIPLE ON AND OFF-SITE TARGETS

A related point is that, following 9/11, the NRC can no longer ignore the very real possibility that an attack on a nuclear power plant would occur commensurate with an attack on other regional infrastructure such as chemical plants and bridges. A coordinated attack designed to effectively eradicate a region would preliminarily target the communication and transportation infrastructures. This will ensure that (A) the region is reduced to mass confusion and (B) law enforcement, and other first responders are impeded from gaining access to the nuclear site. Some areas of the U.S., such as the greater New York

Metropolitan area offer a plethora of target opportunities, with major bridges and transportation arteries being in near vicinity to chemical plants and the Indian Point nuclear power plant (located a mere 25 miles north of New York City). It is imperative that the DBT be modified to mandate a customized approach to high target nuclear facilities like Indian Point.

In addition, the NRC security requirements, must include the following five upgrades:

- (1) The ability of nuclear power plants to fully defend against an attack of the magnitude of 9/11; i.e., 19-20 attackers, attacking a nuclear facility in a coordinated, multi-directional, multi-team attack.
- (2) The ability of nuclear power plants to defend against attacking forces coming by land, water and/or air.
- (3) The ability of nuclear reactors, spent fuel pools and other critical on-site structures to withstand attack by aircraft (including fully-fueled large commercial airplanes and small airplanes or helicopters laden with explosives) as well as the potential aftermath of a massive fuel conflagration.
- (4) The ability of all critical plant structures (including physical security barriers) to withstand an attack by an explosives-laden land vehicle (with the meaning of the term "vehicle" being inclusive of a full range of large vehicles).
- (5) The ability of the plants to defend against attackers utilizing the full range of potential weapons that terrorists are known to be capable of using, including heavy caliber automatic weapons, sniper rifles, shoulder-fired rockets, mortars, anti-tank weaponry, bunker busters, shaped charges, rocket-propelled grenades, high-power explosives, and chemical weapons, as well as cyber-attacks.

Respectfully submitted,

Michel C. Lee, Esq.

Chairman

COUNCIL ON INTELLIGENT ENERGY

& CONSERVATION POLICY (CIECP)

(Home address:

265 Madison Rd.
Scarsdale, NY 10583)

Michael H. Levy
Military Advisor
COUNCIL ON INTELLIGENT ENERGY
& CONSERVATION POLICY (CIECP)

(Home address:
76 Oxford Dr.
Tenafly, NJ 07670)

CC: Michel Lee <ciecplee@optonline.net>

Mail Envelope Properties (43D545D2.4A0 : 1 : 46240)

Subject: NRC Proposed Rulemaking (RIN 3150-AH60) - SUBMISSION OF
COMMENTS ON UPGRADING OF DBT
Creation Date: Mon, Jan 23, 2006 4:07 PM
From: Michel Lee <ciecplee@optonline.net>
Created By: ciecplee@optonline.net

Recipients

nrc.gov
owf5_po.OWFN_DO
SECY (SECY)

Post Office
owf5_po.OWFN_DO

Route
nrc.gov

Files	Size	Date & Time
MESSAGE	9778	Monday, January 23, 2006 4:07 PM
TEXT.htm	24172	
Mime.822	35841	

Options

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

Concealed Subject: No
Security: Standard