(92)

February 21, 2006

Re: NRC Proposed Rule: Design Basis Threat [RIN 3150-AH60]

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

Attn: Rulemakings and Adjudications Staff
Submitted via mail and e-mail to SECY@nrc.gov

COUNCIL ON INTELLIGENT ENERGY & CONSERVATION POLICY (CIECP) COMMENTS TO PROPOSED RULE 10 CFR PART 73 REGARDING THE DESIGN BASIS THREAT FOR SECURITY AT LICENSED NUCLEAR FACILITIES

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.

A January 2005 National Intelligence Council Report describes the terrorist threat to the U.S. as real and as having no sign of abatement for many years to come. This report further warns of a new class of "professionalized" terrorists –in part created by the Iraq war- who must be expected to have strong technical skills and English language proficiency. Such individuals should, in the future, be expected to become major players in international terrorism.

Al Qaeda and other terrorist groups have shown extraordinary tactical ingenuity and a complete lack of reverence for human life. Further there is ample evidence that U.S. nuclear power plants, particularly those sited near metropolitan areas, are viewed as attractive terrorist targets. Notably, the 9/11 Commission learned that the original plan for a terrorist spectacular was for a larger strike, using more planes, and including an attack on nuclear power plants. We also know from the 9/11 Commission's investigation that, even after the plot was scaled down, when Mohammed Atta was conducting his surveillance flights he spotted a nuclear power plant (unidentified by name, but obviously the Indian Point nuclear power plant) and came close to redirecting the strike. In an Al-Jazeera broadcast in 2002, one of the planners of 9/11 said that a nuclear plant was the initial target considered. National Research Council analysis and post-9/11 intelligence has also indicated that the U.S. nuclear infrastructure is viewed as an alluring target for a future terrorist spectacular. As the Chairman of the National Intelligence Council stated in 2004, nuclear power plants "are high on Al Qaeda's targeting list," adding that the methods of Al Qaeda and other terrorist group may be "evolving."

There is, thus, every reason to believe that a sizable, well-planned and orchestrated military operation against a U.S. nuclear facility is well within current terrorist intent and capability.

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

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 documentation) demonstrates that nuclear "insiders" must be deemed potential active participants in an attack.

This threat is significantly augmented by nuclear power plant operators' increasing outsourcing of on-site work in order to cut costs.

Contractor oversight failures have been documented by the NRC. For example a December 22, 2003 NRC Special Inspection Report on the Indian Point Nuclear Generating Station in Buchanan, New York (Indian Point) operated by Entergy Nuclear Northeast (Entergy) notes "the common theme of a lack of direct contractor oversight and quality control measures, along with the absence of Entergy subject matter experts to independently assess contracted work activities...." Critically, the risk of sabotage is elevated at all power plants during periods of refueling and major construction work when hundreds of outside contract workers have site access.

The active participation of insiders, including contract workers, in a terrorist offensive need not take place during the time of attack. It may occur days or even many months prior to an attack. In addition to actions such as surveillance of plant schematics, security features and protocols, pre-attack participation may involve the sabotage of critical instrumentation, computers, piping, 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, viruses and worms. Compromise of integrity may also occur at the level of software development via backdoors written into code or the implantation of logic bombs programmed to shut down a safety system at a particular time.

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 facility. That intrusion disabled a safety monitoring system for nearly 5 hours. In addition, computer hackers have broken into U.S. Department of Energy computers. Some of such intrusions were root-level compromises, indicating that hackers had enough access to install viruses.

Computers at nuclear power stations are also vulnerable to acts of sabotage against off-site power transmission, as was evidenced at Indian Point 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 fully address the potential consequences of the use of toxic chemicals as 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 may also be used strategically to neutralize workers endeavoring to maintain control of the situation.

Many such 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 ascitone methanol can be transported on filter paper, then combined with a heat source to create an explosion.

CONVENTIONAL WEAPONRY

Intelligence and military analysts have repeatedly warned that extremists in Iraq, the tribal areas of Pakistan and elsewhere are currently developing a high level of military skill and experience. This reality underscores the need for nuclear plants to be able to defend against attackers utilizing the full range of potential weaponry that terrorists are known to be capable of using, including heavy caliber automatic weapons; sniper rifles; shoulder-fired rockets; mortars; platter charges; anti-tank weaponry; bunker busters; shaped charges; rocket-propelled grenades; and high-power explosives.

Numerous weapons systems posing a threat to even the best trained and equipped civilian guard force, as well as to on-site installations, are readily available and easy to transport. To wit:

- Assault rifles and other rapid-fire battlefield weapons such as AK-47's, Uzi's and TEC-9's are freely available in the U.S. A weapon like the SKS 7.62-millimenter semiautomatic assault rifle can be purchased for under $200. In 2005 the Government Accountability Office reported that 47 individuals on a federal terrorism watch list were actually permitted to legally buy guns in 2004.

- A standard M-24 sniper rifle with day and night scope can be carried in a canvas bag and fires 7.62-millimeter ammunition targeting up to 3000 feet

- A .50-caliber Barrett rifle, which can be purchased for $1000 on the internet, weighs a mere 30 lbs and can hit targets up to 6000 feet away with armor-piercing bullets that can blow a hole through a concrete bunker, bring down a helicopter or pierce an armored vehicle.

- A rocket propelled grenade launcher is re-loadable, can fire at the speed of 400 feet per second and can blow a vehicle into the air.

- A TOW missile is an accessible form of military hardware used in over 40 countries and can be fired from a launcher on a flatbed truck. A 1998 test TOW fired into a nuclear waste transport cask (which is more robust than many on-site nuclear waste storage casks) blew out a hole the size of a grapefruit. The Kornet-E missile, developed by the Soviets and sold to Iraq, can travel over 3 miles and cut through over 3 feet of steel. The world's arms market is awash in thousands of Milan missiles. The 60-70 lb Milan missile system has an effective range of over 5000 feet and can blow a hole through more than 3 feet of armor plate.

- The deployment of increasingly powerful and sophisticated explosives, including shaped charges, by terrorists and insurgents in Iraq show that the explosives use capabilities of enemies of the United States should not be underestimated. Notably, the 18 men arrested in Australia in November 2005, and believed to have been planning an attack on an Australian nuclear reactor, had allegedly been stockpiling materials used to make the explosive triacetone triperoxide, or TATP. Terrorists targeting a U.S. nuclear power plant may very well be able to draw on expertise developed during the Iraq insurgency as well as military experts and rocket scientists from the former Iraq government or from hostile

nations such as Iran. In addition, the strategic utility of explosives is magnified when bombers are willing to blow themselves up. Suicide bombers able to gain access to the internal areas of a nuclear power plant during the course of an attack could cause untold destruction.

- Perhaps the most intractable military hardware threat is posed by shoulder-fired missiles such as Stingers, SA-7's, SA-14's and SA-18's. An estimated 500,000 such systems are scattered throughout the world and have been found in the possession of at least 27 terrorist or guerrilla groups. Some can be bought easily on the black market for as little as several thousand dollars each. Critically, shoulder-fired missiles are easy to operate (Al Qaeda training videos offer instruction) and are designed for portability, typically being 5-6 feet long and weighing 35 lbs. They can be transported by and fired from a van, S.U.V., pickup truck or recreational boat. Even a single terrorist armed with a shoulder-fired missile can cause immediate and substantial damage to a targeted structure. Traveling at more than 1,500 miles per hour, a typical shoulder-launched missile has a range of over 12,000 feet. If the target remains intact following the initial strike, the terrorist can attach a new missile tube to the grip stock launcher and fire again.

WATERBORN ATTACKS

Waterborne defenses must be added to nuclear plants adjacent to navigable waterways. Facilities must either be engineered to withstand damage from a waterborne attack or suited with physical barriers that prevent entry to the plant and/or critical cooling intake equipment.

Continual cooling is an essential component of nuclear plant safety. A meltdown can be triggered even at a scrammed reactor if cooling is obstructed. Water intake is also essential to the proper function of spent fuel pools. Yet at certain nuclear plants, cooling systems may be highly vulnerable. At both Indian Point and Millstone Power Station, in particular, water intake pipes have been identified by engineering experts as exposed and susceptible to waterborne sabotage.

One or more boats laden with high energy explosives could severely compromise cooling water intakes easily and quickly. Indian Point, for instance, is located on the banks of the Hudson River in an area heavily trafficked by commercial and recreational vessels. The 900 foot "Exclusion Zone" –marked only by buoys- could be traversed by speed boats in 30 - 40 seconds, well before any Coast Guard or other patrol boat could react. Patrol boats could also be readily taken out by suicide bomber boats crashing into them (in the manner a small explosives laden boat targeted the destroyer the USS Cole in 2000) or by weaponry like shoulder-fired missiles or rocket propelled grenades.

AERIAL ASSAULT

According to a terrorist "threat matrix" issued by the National Research Council and the National Academies of Sciences and Engineering following the September 2001 attack,

"Nuclear power plants may present a tempting high-visibility target for terrorist attack, and the potential for a September 11-type surprise attack in the near term using U.S. assets such as airplanes appears to be high."

In March 2005, a joint FBI and Department of Homeland Security assessment stated that commercial airlines are "likely to remain a target and a platform for terrorists" and that "the largely unregulated" area of general aviation (which includes corporate jets, private airplanes, cargo planes, and chartered flights) remains especially vulnerable. The assessment further noted that Al Qaeda has "considered the use of helicopters as an alternative to recruiting operatives for fixed-wing operations," adding that the maneuverability and "non-threatening appearance" of helicopters, even when flying at low altitudes, makes them "attractive targets for use during suicide attacks or as a medium for the spraying of toxins on targets below."

The vulnerability of nuclear power plants to malevolent airborne attack is detailed extensively in the Petition filed by the National Whistleblower Center and Randy Robarge in 2002 pursuant to 10 CFR Sec. 2.206. A number of studies of the issue are also reviewed in Appendix A to these Comments. The particular vulnerability of nuclear spent fuel pools to this kind of attack is detailed in the January 2003 report of Dr. Gordon Thompson, director of the Institute for Resource and Security Studies entitled "Robust Storage of Spent Nuclear Fuel: A Neglected Issue of Homeland Security" and in the findings of a multi-institution team study led by Frank N. Von Hippel, a physicist and co-director of the Program on Science and Global Security at Princeton University and published in the spring 2003 edition of the Princeton journal *Science and Global Security* under the title "Reducing the Hazards from Stored Spent Power-Reactor Fuel in the United States." It is worthy of note that, even post-9/11, general aviation aircraft have circled or flown closely over commercial nuclear facilities without military interception.

The NRC's sole present strategy for averting a kamikaze attack upon a nuclear power plant is reliance upon aviation security upgrades implemented by the Transportation Security Administration and the Federal Aviation Administration and faith that U.S. intelligence will provide ample warning. It is this kind of governmental agency pass-the-buck mindset that brought the nation Katrina.

(The NRC's conjecture also betrays a reality disconnect reminiscent of the federal response to Katrina. Since 2001 there have been numerous breaches of airport security throughout the nation. Notably, in late 2005, there were three serious security breaches at Newark International Airport, one of the points of departure used by the September 11 hijackers. The most serious occurred on November 12, 2005, when a man driving a large S.U.V. barreled through the armed security checkpoint and drove in a secured area for 45 minutes before being found by NY/NJ Port Authority officers.)

The DBT must be upgraded to include high-speed attack by a jumbo jet of the maximum size in commercial use and smaller general aviation aircraft and helicopters. The DBT must assume all such aircraft are fully loaded, fueled and carry explosives.

It is essential that the DBT address not only the direct effect of impact, but the full potential aftereffects of (A) induced vibrations; (B) dislodged debris falling onto sensitive equipment; (C) a fuel fire; and (D) the combustion of aerosolized fuel (especially in combination with pre-existing on-site gases such as hydrogen).

The DBT must further take into consideration the cascading consequences of aerial assault on the full spectrum of plant installations. Inarguably, there is a wide range of on-site structures, not within hardened containment, that are critical to the safe operation of a nuclear plant. Spent fuel pools are of particular concern because the disposition of water could uncover the fuel. If plant workers are unable to effectuate replacement of the water (either because of fire or because they are otherwise incapacitated), experts warn, an exothermic reaction could cause the zirconium clad spent fuel rods to ignite a nuclear waste conflagration that would very likely spew the entire radioactive contents of the spent fuel pool into the atmosphere.

Without question, hardening a nuclear power plant against aerial threat will necessitate significant upgrades in plant fortification. However even relatively modest measures such as the installation of Beamhenge and the placement of all sufficiently cooled spent fuel into Hardened On-Site Storage Systems (known as HOSS) would add measurable protection.

STRATEGIC USES OF RIGS, TRUCKS AND S.U.V.'S

In June 1991, the NRC denied the truck bomb petition of the Committee to Bridge the Gap and the Nuclear Information Resource Service, on the grounds that it was not realistic to believe a truck bomb would be employed in the U.S. Two years later, on February 26, 1993, terrorists drove a rented van packed with explosives into the underground garage of the World Trade Center, lighted a fuse and fled. Just a couple of weeks before that, a mentally unstable individual crashed his station wagon through the gates of the protected area of the Three Mile Island nuclear power station and evaded security for several hours before finally wrecking his vehicle by crashing into the turbine building. Thereafter, the NRC reconsidered its earlier assessment and upgraded the DBT to include some protections against land vehicles. Such upgrades, however, are insufficient in a post-9/11 world.

Large Sport Utility Vehicles and pickup trucks on the road today can weigh over 8 tons, loaded, and -as do commercial vans- have considerably carrying capacity. Such vehicles could be used strategically in a number of ways.

The first is as a mobile short range projectile bomb. A large, heavy vehicle packed with high explosives, even if not successful in penetrating concrete barriers, could result in the death or incapacitation of large numbers of plant workers, including security, personnel. Such casualties would be particularly likely to materialize if the vehicle bomb followed a previous diversionary event intended to draw security personnel to the plant perimeter.

The second is as a transport vehicle for one team of attackers who are themselves armed or who wear explosive belts and could then themselves penetrate other areas of the facility. (A terrorist wearing an explosive body belt can, in effect, be a precision guided weapon.)

The third and fourth scenarios are variations of the first two, with chemical agents substituted for explosives. One or two such vehicles packed with the right toxins, could be expected to kill or disable a substantial number of workers, again, especially if the

release followed a prior event which drew security personnel to the area, or simply to areas outside facility enclosures. (A toxin like Chlorine gas can be lethal to anyone within miles.) Attackers wearing protective gear might then be able to gain access to other areas of the facility.

A fifth tactical use of vehicles would not even occur on site. Vehicles carrying explosives and/or chemical agents could be set off at critical regional transportation arteries such as major bridges, tunnels and highways. Notably, such incidents could be staged in a way that would not even alert authorities to the onset of terrorist activity. In the New York metropolitan region in which Indian Point is sited, for example, a series of major accidents occurring at or about the same time would not be an unusual occurrence. In fact, on July 25, 2003, the very day the Federal Emergency Management Agency declared that the Indian Point emergency plan provided "adequate" assurance of protection to the public, the entire New York metropolitan region was brought to a virtual traffic standstill after a tractor-trailer hit a beam on the George Washington Bridge and burst into flames, several minor accidents and a car fire took place on Interstate 95, and a truck got jammed under an overpass of the Hutchinson River Parkway. Just last month, a tanker truck carrying 8000 gallons of gasoline overturned on one of New York City's busiest highways, igniting a blaze that burned for hours and weakening the steel beams of a bridge above.

The staging of a couple of incidents like those just noted, combined with an "accident" involving a tanker carrying hazardous gasses or liquids like liquefied ammonia, chlorine, propane or vinyl chloride, prior to an assault would almost assuredly forestall the provision of outside assistance to a nuclear facility under attack.

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

Whether or not an attack employs strategies designed to obstruct regional transportation routes, 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 Indian Point is sited – roadway logistics and regular congestion alone would likely prevent assisting forces from reaching a nuclear plant under attack in time. (It bears mention that SWAT team assembly takes approximately 2 hours, whereas an assault could be over in a matter of minutes.)

It is accordingly crucial that the NRC cedes the faulty assumption that plant personnel need only fend 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".

ELEVATED VULNERABILITY TO INFILTRATION DURING EVENT

During a crisis event at a nuclear plant there also exists an elevated threat of infiltration by terrorists posing as first responders or National Guard. And in fact the imposter tactic has been used by terrorists in recent years with substantial success.

Terrorists disguised as firefighters could take particularly strong advantage of this stratagem. Outside firefighters often respond to fires at nuclear power plants and many attack scenarios would be expected to involve fire. Firefighters would presumptively be seen as benign by plant personnel and would have a legitimate reason to move throughout a facility and "check" components such as electrical wiring. Moreover, bulky firefighter uniforms and equipment can hold and hide a host of articles that could be used for destructive purposes.

DEFENSE AGAINST A SIZABLE MULTI-TEAM, MULTI-DIRECTIONAL FORCE

In January 1991, the Committee to Bridge the Gap and the Nuclear Information Resource Service filed a joint Petition with the NRC requesting, *inter alia,* that the DBT be upgraded to 20 external attackers. The NRC rejected the petition in June 1991, asserting that an attack involving more than 3 assailants was unrealistic.

September 11 was a demonstration in the limitations of governmental foresight.

The September 11 plot involved 20 attackers (although only 19 were ultimately able to participate). The tragic 2004 siege at a school in Belsan, Russia involved more than 30 armed terrorists. It should be beyond question at this point that a terrorist attack could involve scores of attackers.

Accordingly, the DBT must assume at least two dozen attackers. Lessons learned from 9/11 and the many multiple coordinated terrorist actions that have transpired in Europe, Asia and the Middle East since then, also mandate the premise that attackers will act in several teams.

Any carefully planned attack on a nuclear facility by knowledgeable individuals, would also involve several different *modus operandi.* The DBT should therefore take into account the consequences of near-simultaneous damage to different plant installations, systems and personnel (e.g., the effect of a small explosive-laden plane diving into the roof of a spent fuel pool coupled with the waterborne sabotage of the spent fuel pool intake system).

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 very likely preliminarily target communication, electrical power and/or transportation

infrastructures. This would ensure that (A) the targeted region is reduced to mass confusion, (B) local and federal officials and responders would be overwhelmed, and (C) law enforcement and other first responders would be impeded from gaining access to the nuclear plant site.

Certain areas of the U.S. offer a plethora of target opportunities and thus are particularly vulnerable to multiple target scenarios. Prime among them is the greater New York Metropolitan area (already in the terrorists' crosshairs) which contains numerous national landmarks, corporate headquarters, reservoirs, bridges, airports, transportation arteries and hazardous chemical plants, all in near vicinity to Indian Point, a mere 24 miles north of New York City.

A CREDIBLE NUCLEAR PLANT SECURITY FORCE TESTING PROGRAM

The deficiencies, failures, and chicanery that have long plagued the various manifestations of the nuclear power industry security drills and force-on-force (FOF) testing have been exhaustively documented in recent years. Noteworthy investigations in this regard have been conducted by the Project on Government Oversight (augmented by testimony provided in 2002 Senate Environment and Public Works Committee hearings) and the United States General Accounting Office (which reported its findings in a September 2003 report entitled "Oversight of Security at Commercial Nuclear Power Plants Needs to Be Strengthened") as well as by the press. Problems with the FOF program are also addressed in the July 2004 Petition for Rulemaking to amend 10 CFR Part 73 to upgrade the DBT filed by the Committee to Bridge the Gap and the Comments on the DBT recently filed in January 2006 by the Union of Concerned Scientists. CIECP endorses the recommendations made by the Committee to Bridge the Gap and the Union of Concerned Scientists fully.

CIECP urges the NRC in the strongest possible terms to upgrade drills and testing protocols to remedy the flaws that are a matter of public record and to take into account the realities noted herein. FOF tests must be sufficiently challenging to provide high confidence in the defensive capabilities of the security forces at the nation's 103 nuclear power plants. One clear failing of the FOF program to date has been the giving of excessive warning regarding upcoming tests. While some notice is necessary, one week should suffice. In addition, staff assignments should be frozen on the day of notice. This would eliminate the all too common practice of substituting a plant's most fit and accomplished security personnel in place of underachievers.

It is also critical that drills and the FOF program be revamped to eliminate the ongoing conflicts of interest inherent in (1) The NRC allowing the nuclear industry's lobbying arm, the Nuclear Energy Institute (NEI) to award the FOF contract; and (2) The NEI, with NRC approval, then selecting Wackenhut, a corporation which contracts security guards to nearly half the nuclear power plants in the U.S., to also be the contractor that supplies the mock adversary teams for the FOF tests.

Such problems have reduced the value of testing to the point where the FOF program lacks public confidence. The program must be redesigned and monitored by an independent entity such as the very capable U.S. military.

HIGH TARGET APPEAL REACTORS

Prior terrorist attacks and plots against the U.S. have focused on major cities. It is a matter of fundamental logic that plants sited in highly populated metropolitan areas, particularly those with high symbolic value, face the greatest risk of being selected as a target.

It is thus imperative that the DBT be modified to mandate a customized approach to high target nuclear facilities.

SITE-SPECIFIC SAFETY-RELATED VULNERABILITIES

It is highly unrealistic to exclude from the DBT calculus the reality of deteriorated conditions and compromised systems that exist at various nuclear power plants in the U.S. A facility-customized approach must be taken which adds problems which are known or reasonably suspected and which could have a significant effect upon the ability of plant operators to maintain control during a major incident into the security equation.

Prime among factors which may be site-specific are:

- Corrosion and Embrittlement: For example, a risk of corrosion of the steel liner of the reactor containment at the Oyster Creek Nuclear Generating Station (Oyster Creek) was recently identified. A qualified corrosion expert has warned that the risk may be high enough to cause buckling and collapse. Manifestly, corrosion or embrittlement-weakened structures and components are more vulnerable to the effects of heat and combustion.

- Vulnerability to Fire: Fire detection and suppression equipment and fire barriers are crucial to reactor safety. Over 20 years ago a worker at the Brown's Ferry Unit 1 reactor accidentally started a fire which destroyed emergency cooling systems and severely compromised the plant's ability to monitor its condition. In response, the NRC increased fire safety standards. Recently, the NRC has effectively relaxed those standards. This is exceedingly unwise. During the chaos and threat level that would surely exist during a terrorist attack, human beings cannot be presumed to be able to take the actions necessary to protect critical systems from fire. The systems themselves must have integral safeguards. Yet plants such as Arkansas Nuclear One, Catawba, Ginna, H.B. Robinson, Indian Point, James A. Fitzpatrick, McGuire, Shearon Harris, Vermont Yankee and Waterford have been identified as having fire barrier wrap systems that failed fire tests. Fireproofing problems such as these jeopardize safe shutdown and must be recognized as a degradation of defense-in-depth protection. In addition, any plant fire hazard analyses must assume damage to multiple rooms and multiple structures, a circumstance that could easily result from an aircraft impact.

- Integrity of Structures that Support Mobility: While the focus of NRC regulatory review is on structures and equipment directly related to safe operational

function, the conditions that may prevail during an assault would likely require plant personnel to be able to move rapidly throughout the facility. The evaluation of the reliability of structural features such as stairways (which might buckle or melt during a fire) is accordingly critical.

- Electrical System Problems: In 2003, a cable failure knocked out power to approximately half the safety systems at Oyster Creek, including security cameras, alarms, sensors, pumps and valves. In February 2003, all 4 of the backup generators at Fermi became simultaneously inoperable. In December 2001, Indian Point reactor 2 lost power due to a malfunction of the turbine, then lost back-up power to the reactor coolant system because of a second electrical failure. During the August 2003 blackout that struck the Northeast, following the loss of off-site power, two of Indian Point's emergency backup generators (both of which had been previously flagged as having problems) failed to operate. In view of the severe consequences failures such as these could have were they to occur during a major incident, known plant electrical system vulnerabilities must be taken into consideration.

- Cooling System Problems: Cooling system problems and design deficiencies have plagued a number of plants in recent years. In some cases the NRC has allowed plants to operate for long periods with compromised emergency cooling systems. For example, the Salem nuclear power station had experienced two years of repeated malfunctions of its high-pressure coolant-injection system prior to the time, in October 2003, when operators unsuccessfully tried to use it to stabilize water levels following a steam pipe burst. And the NRC has allowed reactors with emergency sump pumps flagged as likely to become clogged and inoperative to remain in operation for many years without repair. The Los Alamos National Laboratory, for instance, concluded that the sump pumps at Indian Point reactors 2 and 3 could become clogged in as little as 23 minutes and 14 minutes, respectively. Either the NRC should mandate immediate correction of cooling system vulnerabilities such as these or it must deem them a constituent element of site-specific DBT analyses for the duration of the system's functional declination.

ELIMINATE COMMERCIAL CONSIDERATIONS FROM THE DBT CALCULUS

The commercial interests of the nuclear industry are of valid concern to nuclear utilities and the NEI; they should not be of concern to the NRC. There is no justification for jeopardizing national security and the health and safety of the public - even to the smallest degree – to safeguard corporate profits.

The NRC states in the proposed rule that the DBT is based upon the analysis of the largest threat against which a "**private security force could reasonably be expected to defend**" [*emphasis added*] 70 FR 67385.

Both the NRC and the industry have acknowledged that, in their estimation, a private guard force should not be reasonably expected to defend against a 9/11-type attack involving aircraft. Such an attack, apparently, is deemed to fall under the loophole of 10

CFR Sec. 50.13, which exempts reactor operators from defending against "an enemy of the United States, a foreign government or other person". The perimeter of this "enemy of the United States provision has never been defined, so there is no way to know how far it extends. However, it is abundantly clear from the public record that the NRC has drawn the line at point where the profit margins of nuclear power operators might be significantly affected. Unfortunately, the terrorists are constrained by no such boundary.

Congress has charged the NRC with the obligation to protect the public health and safety. This must not be viewed as a mandate; it must be viewed as an uncompromised mandate.

If the NRC does not believe its licensees can afford the security upgrades necessary to protect the nation's nuclear reactors against the full potential threat, it must act with forthrightness and publicly demand that the Department of Homeland Security or the U.S. military assume responsibility for domestic nuclear power plant security.

CONCLUSION

The 9/11 Commission observed: "Across the government, there were failures of imagination, policy, capabilities...The most important failure was one of imagination. We do not believe leaders understood the gravity of the threat."

As a public interest group we ask: What needs to happen before the gravity of the threat is not only understood, but acted upon?

Respectfully submitted,

COUNCIL ON INTELLIGENT ENERGY
& CONSERVATION POLICY

By

Michel C. Lee, Esq.
Chairman

(914) 393-2930

Michael H. Levy
Military Advisor

APPENDIX A

Since September 11, 2001, there has been much speculation about the vulnerability of nuclear power plants to aerial attack. Certainty, however, is in short supply.

What is known is that none of the nuclear reactors presently operational in the United States were built to withstand the crash of a jumbo jet. Studies that have addressed the issue include the following:

1974: To date the only published peer reviewed study on the vulnerability of U.S. nuclear power plants was conducted by General Electric, the leading builder of nuclear plants, and published in the industry journal *Nuclear Safety.* GE looked at accidents – not terror attacks – and concluded that were a "heavy" airliner to hit a reactor building in the right place, it would almost certainly rip it apart. Such a hit would also most likely damage the reactor core and both the cooling and emergency cooling systems. [NOTE: The GE study defined a "heavy" plane as one weighing more than 6 tons. The Boeing 757 which gouged a 100 foot gash through the reinforced concrete of the Pentagon weighed between 80 and 100 tons. A fully loaded 767 weighs over 200 tons. The Airbus 380, expected to be launched into commercial use later this year, takes to the air weighing 1.2 million pounds, hundreds of thousands of pounds heavier than the Boeing 747, the current jumbo of the sky.]

1982: A technical report (previously publicly available) of a study conducted by the U.S. Army Corps of Engineers at the NRC's behest focused on plane crash analyses at the Argonne National Laboratory. The Corps concluded that planes traveling at a speed of over 466 mph would crash through the average reactor containment structure noting "account has been taken of the internal concrete wall which acts as a missile barrier...It would appear, however, that this is too optimistic since vaporized fuel, hot gaseous reaction products, and to a certain extent portions of liquid fuel streams will flow around such obstructions and overwhelm internal defenses...." [NOTE: An FBI analysis estimated that American Airlines Flight 11, which hit the north tower of the World Trade Center, was traveling at a speed of 494 mph, and that United Airlines Flight 175, which hit the south tower, was traveling at 586 mph, a speed far exceeding its design limit for the altitude.]

2000: A NRC study published less than a year before September 11 calculated that 1 out 2 commercial airplanes flying in the year 2000 were large enough to penetrate even a 5 foot thick reinforced concrete wall 45% of the time. Specifically, the study states, "aircraft damage can affect the structural integrity of the spent fuel pool or the availability of nearby support systems, such as power supplies, heat exchangers, or water makeup sources and may also affect recovery actions...It is estimated that half the commercial aircraft now flying are large enough to penetrate the 5 foot thick reinforced concrete walls." [NOTE: The thickness of the top of certain reactor domes is 3 and-a-half feet.]

2002: The German Reactor Safety Organization (GRS) a scientific-technical research group that works primarily for nuclear regulators in Germany conducted an extremely detailed study that determined that terrorists can, with a strategically targeted airplane crash, initiate a nuclear accident. (A secret Ministry document that summarized the report was leaked to the German and Austrian press and subsequently translated into English.) The GRS study used dynamic computation modeling that looked at the

potential consequences of a wide range of impact possibilities on different plant equipment and installations. Different types of airplanes, velocities, angles of impact, weight loads and fuel effects were considered, as were various sequences of events. Aside from the basic finding of vulnerability, the GRS study is significant for recognizing the limitations of even its highly complex analyses. Key unknowns include the impacts of fire loads on many kind of materials and equipment as well as the behaviors of various combustive materials under the conditions of a plane crash.

2004: In 2004 the U.K. Parliamentary Office of Science and Technology (OST) issued a secret report on the risks of terrorist attacks on nuclear facilities to the U.K. House of Commons Defense Committee. The OST report was leaked to the magazine *New Scientist*, which reported the OST conclusion that a large plane crash into a nuclear reactor could release as much radiation as the1986 accident at Chernobyl, while a crash into the nuclear waste tanks at the U.K.'s Sellafield facility could cause several million fatalities.

From these studies it is clear that there exists a reasonable basis for concern regarding malevolent deployment of aircraft against nuclear power facilities. It should also be evident that all studies on this topic are, in substance, educated conjecture. The current state of computer modeling is not up to analyzing the full range of physical and chemical interactions that could occur under the incalculable range of different kinds of aircraft, approaching at different angles, at different speeds, hitting different structures, which all have facility-unique room and equipment layouts, and different substance, chemical, and ventilation-related conditions. A lesson in the unpredictable consequences of airplane crashes was brought home on September 11 (when even the 47 story tall 7 World Trade Center that was not struck collapsed for reasons engineers have still not fully determined). A lesson in the limitations of advanced computer modeling can also be learned from the Columbia space shuttle disaster.

From: Michel Lee <ciecplee@optonline.net>
To: <SECY@nrc.gov>
Date: Tue, Feb 21, 2006 2:51 PM
Subject: NRC Proposed Rulemaking (RIN 3150-AH60) Submission of Updated Comments on Upgrading of DBT

Re: NRC Proposed Rule 10 CFR Part 73: DBT (RIN 3150-AH60)

February 21, 2006

Annette Vietti-Cook, Secretary

U.S. Nuclear Regulatory Commission

Washington, DC 20555-0001

ATTN: Rulemakings and Adjudications Staff

Below and attached are the comments on the proposed Design Basis Threat rulemaking submitted on behalf of the Council on Intelligent Energy & Conservation Policy (CIECP).

These comments are intended to supercede the comments of CIECP filed in January, prior to the extension of the time for comments submission to February 22, 2006.

Council on Intelligent Energy

& Conservation Policy (CIECP)

by:

Michel Lee, Esq.

Chairman

(914) 393-2930

ciecplee@optonline.net

[home address:

265 Madison Rd.

Scarsdale, NY 10583]

Michael H. Levy

Military Advisor

[home address:

76 Oxford Dr.

Tenafly, NJ 07670]

February 21, 2006

Re: NRC *Proposed Rule: Design Basis Threat* [RIN 3150-AH60]

Secretary

U.S. Nuclear Regulatory Commission

Washington, DC 20555-0001

Attn: Rulemakings and Adjudications Staff

Submitted via mail and e-mail to SECY@nrc.gov

Mail Envelope Properties (43FB6F31.CD7 : 10 : 7383)

Subject:	NRC Proposed Rulemaking (RIN 3150-AH60) Submission of Updated Comments on Upgrading of DBT
Creation Date:	Tue, Feb 21, 2006 2:50 PM
From:	Michel Lee <ciecplee@optonline.net>
Created By:	ciecplee@optonline.net

Recipients
nrc.gov
owf5_po.OWFN_DO
SECY (SECY)

Post Office	**Route**
owf5_po.OWFN_DO	nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	45925	Tuesday, February 21, 2006 2:50 PM
TEXT.htm	115468	
CIECP Comments on DBT version 2.doc	126976	
Mime.822	338237	

Options

Expiration Date:	None
Priority:	Standard
Reply Requested:	No
Return Notification:	None
Concealed Subject:	No
Security:	Standard