

Union of Concerned Scientists

Citizens and Scientists for Environmental Solutions

TESTIMONY SUBMITTED BY
EDWIN S. LYMAN, PH.D.
SENIOR SCIENTIST, GLOBAL SECURITY PROGRAM
TO THE
SUBCOMMITTEE ON CLEAN AIR, CLIMATE CHANGE AND NUCLEAR SAFETY
COMMITTEE ON ENVIRONMENT AND PUBLIC WORKS
UNITED STATES SENATE
MAY 26, 2005

Mr. Chairman and members of the Subcommittee, on behalf of the Union of Concerned Scientists, I would like to thank you for the opportunity to present our views on the effectiveness of the Nuclear Regulatory Commission (NRC) in overseeing the security and safety of nuclear power plants in the United States.

My name is Edwin Lyman. I have been a Senior Scientist with the Global Security Program at the Union of Concerned Scientists (UCS) since May 2003, focusing on ways to prevent nuclear proliferation, nuclear terrorism and radiological terrorism. I have been working on these issues for fourteen years. Prior to my current position, I was with the Nuclear Control Institute for seven years, and served as its president from 2002-2003. I received a PhD in physics from Cornell University in 1992, after which I did three years of postdoctoral work at Princeton, analyzing issues at the intersection of nuclear nonproliferation, nuclear safety and environmental protection.

I am testifying today as a public interest advocate in an unusual position. As the result of my participation in an NRC hearing on security issues at a nuclear power plant in South Carolina, I have had access both to site-specific security information and to general information pertaining to the NRC's post-9/11 security policies. I cannot discuss that information here in open session,

Washington Office: 1707 H Street NW Suite 600 • Washington DC 20006-3919 • 202-223-6133 • FAX: 202-223-6162
Cambridge Headquarters: Two Brattle Square • Cambridge MA 02238-9105 • 617-547-5552 • FAX: 617-864-9405
California Office: 2397 Shattuck Avenue Suite 203 • Berkeley CA 94704-1567 • 510-843-1872 • FAX: 510-843-3785

although I would welcome the opportunity to do so at some future time in a closed forum. However, I am able to say that my long-standing concerns about security at NRC-regulated facilities have by no means been alleviated by what I have learned.

As I will discuss, UCS has two basic concerns about security at U.S. nuclear facilities in the post-9/11 world. 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 vulnerable to terrorist attacks that could result in the release of significant radiation—far more deadly than any "dirty bomb."

What I find most troubling is that I see little evidence of "outside-the-box" thinking going on in the NRC or in the industry in response to emerging threats or safety concerns. They do 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 I doubt that America's adversaries put similar constraints on themselves when plotting attacks.

The NRC has become too self-satisfied with the way it does business, too evasive about potential hazards, too unresponsive to external criticism, and too close to the industry that it regulates. Stringent oversight of the NRC by Congress and independent non-governmental groups is essential to counterbalance the lax regulation and enforcement that can result from complacency and to ensure that the NRC can effectively protect public health and safety. Congressional action in the security area is especially important, because the American public cannot directly participate in the discussion and has little other recourse for ensuring that the government is doing everything it can to protect it from nuclear and radiological terrorism. To this end, legislation is needed to ensure that there is independent review of NRC policy decisions pertaining to the protection of America's commercial nuclear facilities against both radiological sabotage and theft of weapon-usable materials.

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. Only last month, 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 in our judgment, 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 teach Russia to better protect its own weapon-usable material. We would urge the Congress to take a closer look at these issues.

Terrorist Attacks on Nuclear Power Plants and Their Consequences

More than three 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 terrorists were to succeed in gaining forced entry to a

nuclear power plant, within a matter of minutes it could do enough 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 public has a right to know about the dangers that they may face from plants in their vicinity, and the NRC has a responsibility to ensure that emergency planning is based on the most accurate information and is conservative enough to provide ample protection. But the NRC is doing a disservice to the public by making misleading and confusing statements about the potential consequences of terrorist attacks or severe accidents at nuclear plants. It has backed away from its own publicly available pre-9/11 radiological assessments, and claims that more recent analyses show that there is much less cause for concern. But the public must take these claims on faith, because the new assessments are all classified.

After the 9/11 attacks, the NRC repeatedly asserted that the public had little to fear from a jumbo jet attack on a nuclear plant, because of the plants' redundant safety systems, highly trained operators, robust structures, and emergency procedures. But the NRC admitted that it had never analyzed such attacks, so it commissioned classified vulnerability assessments from the national laboratories to determine what could actually happen.

After these studies were completed, the NRC then conceded that there was a small chance that such an attack could cause a radiological release, but maintained that the NRC's "emergency planning basis" would remain valid.[1] However, the NRC's emergency planning basis already includes, in principle, consideration of severe, Chernobyl-type accidents involving core melt and containment failure. So all the NRC's statement actually says is that a 9/11-style attack on a nuclear plant wouldn't cause an event worse than Chernobyl, which is not very reassuring. And, as I discuss below, in the event that such a calamity occurs, NRC's emergency planning procedures may help to limit the near-term deaths from acute exposure to radiation, but would

[1] Statement submitted by Luis Reyes, U.S. Nuclear Regulatory Commission, to the Subcommittee on National Security, Emerging Threats and International Relations, Committee on Government Reform, U.S. House of Representatives, September 14, 2004, p. 8.

have little impact on the large numbers of cancer fatalities that could result from lower but still significant exposures to the radioactive plume.

The effects of such attacks would be particularly severe for nuclear plants situated in densely populated metropolitan areas and near nerve centers of our economy, such as Indian Point, only 25 miles north of New York City. A study that I prepared last year for the environmental group Riverkeeper found that the consequences of a terrorist attack at one of the reactors at Indian Point could be catastrophic, with up to 44,000 deaths in the near-term from acute radiation poisoning, 500,000 deaths in the long-term from cancer, and economic damages that could exceed $2 trillion.[2] It is hard to conceive of a "dirty bomb" that could do as much damage. This study was performed using the same computer codes and radiological releases ("source terms") that NRC itself uses for conducting radiological assessments.

Another notable finding of the Indian Point study is the widespread extent of the contamination that can result from a nuclear plant attack. The calculations clearly showed that severe health consequences can occur at locations far downwind of the affected plant, with near-term fatalities occurring up to 60 miles away. An attack on Indian Point could be catastrophic not only for New York City but also for densely populated parts of New Jersey and Connecticut.

Perhaps the most troubling result of the study involved the doses to children from radioactive iodine exposure. Radioactive iodine can concentrate in the thyroid, delivering very high radiation doses to thyroid tissue and posing an elevated risk of thyroid cancer, particularly in children. One of the terrible legacies of the 1986 Chernobyl accident is the epidemic of thyroid cancer among children exposed to radioactive iodine, a causal relationship that has now been conclusively established.[3]

Potassium iodide (KI), if administered within a few hours of exposure to radioactive iodine, can be very effective in reducing the radiological impact. NRC's policy is to provide funds for purchase of KI, in states that request it, for individuals within the roughly circular, 10-mile-

[2] Edwin S. Lyman, "Chernobyl-on-the-Hudson? The Health and Economic Impacts of a Terrorist Attack at the Indian Point Nuclear Plant," commissioned by Riverkeeper, Inc., September 2004.
[3] E. Cardis et al., "Risk of Thyroid Cancer After Exposure to ^{131}I in Childhood," *Journal of the National Cancer Institute* **97** (2005) 724-32.

radius "plume exposure" emergency planning zone (EPZ). However, the results of the Indian Point study indicate that children hundreds of miles away from a nuclear power plant attack could receive exposures to the thyroid in excess of 5 rem, the dose that would trigger administration of KI under FDA guidelines. The current NRC policy appears to leave many children at serious risk in the event of a severe accident or terrorist attack at a nuclear plant.

The NRC's position is that there is no need for KI distribution more than ten miles away from any nuclear plant. But although the NRC doesn't like to point this out, this assessment is appropriate only for accidents in which the containment building remains intact and significantly reduces radiological releases to the environment. In the post-9/11 era, such an assumption should no longer form the basis for emergency planning decisions, given that terrorists capable of attacking a plant and causing a meltdown would also likely be able to breach the containment as well. A more prudent KI policy should be based on a more realistic radiological assessment that considers containment breach events and uses plume mapping, based on site-specific meteorological conditions, to determine the regions where KI is likely to be needed.

These dangers are not exclusive to plants in urban areas like Indian Point. Over the last fifteen years, suburban sprawl has led to substantial population growth in rural areas, some of them near formerly remote nuclear power plants. Preliminary UCS data based on U.S. Census figures indicate that between 1990 and 2000, the number of people living within the 10-mile emergency planning zones of many nuclear plants, including Calvert Cliffs in Maryland, Catawba in South Carolina, North Anna in Virginia, Shearon Harris in North Carolina and Comanche Peak in Texas, increased by 35% or more from 1990-2000 — nearly three times the average population growth of the nation during that period.

Moreover, the attack scenario evaluated in the Indian Point report was far from the worst case. For instance, the study assumed that the attack only caused damage to the reactor itself and not to the spent fuel pools, which remained fully functional after the attack. However, the spent fuel pools themselves contain enormous quantities of long-lived radionuclides, are not protected by containment buildings like the reactors themselves, and are vulnerable to zirconium cladding fires and fuel melting in the event of an extended interruption to their active cooling systems. As

the recent National Academy of Sciences study on spent fuel pool risks has made clear, a terrorist attack on a spent fuel pool could, under some conditions, lead to the release of large quantities of radioactive materials to the environment.[4] Calculations that I performed for an article published last year in the Princeton-based journal *Science and Global Security* showed that a terrorist attack on a spent fuel pool alone could result in thousands of cancer deaths and economic damages in the range of hundreds of billions of dollars.[5]

Preventing Terrorist Sabotage Attacks and Thefts of Nuclear Materials

There are several ways in which the NRC can strengthen its regulations for protecting the public from the threats of sabotage attacks on nuclear power plants and thefts of nuclear weapon-usable materials from Category I nuclear facilities. These include: (1) insuring that the "design basis threats" that facilities are required to protect against adequately represent the terrorist threats that those facilities actually face; (2) ensuring that force-on-force tests used to assess the adequacy of security measures at nuclear facilities are realistic and credible; (3) addressing the continuing problem of guard fatigue at nuclear plants; (4) reforming the implementation of "risk-informed regulation" to allow an increase in regulatory burdens when warranted; and (5) imposing the same standards for safety culture at the NRC as the NRC does for nuclear plants. I discuss each of these in turn below.

Design Basis Threat (DBT)

The DBT is a description of the size 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). In April 2003, after a long deliberative process, the NRC issued revised DBTs to take into account the increased threat environment after the 9/11 attacks.

[4] Board on Radioactive Waste Management, National Research Council, "Safety and Security of Commercial Nuclear Fuel Storage," Public Report, National Academies Press, Washington, D.C., 2005, Executive Summary, p.6.

[5] J. Beyea, E. Lyman, F. von Hippel, "Damages from a Major Release of ^{137}Cs into the Atmosphere of the United States," *Science and Global Security* **12** (2004) 125-136.

Nuclear power plant licensees and Nuclear Energy Institute officials were allowed to review and comment on the proposed radiological sabotage DBT, 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 were not very happy with the proposal. As 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 …"[6]

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."[7] 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

[6] NRC Commissioner Edward McGaffigan, personal communication, May 16, 2003.
[7] "NRC Approves Changes to the Design Basis Threat and Issues Orders for Nuclear Power Plants to Further Enhance Security," press release, April 29, 2003.

Plan, which was issued in interim form in February of this year, are a long way from being implemented.

While it is reasonable not to include members of the public in 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.[8]

The NRC's current plan to revise its physical protection regulations through a rulemaking presents an opportunity to increase the transparency of its security decision-making, but only if the NRC makes every effort to maximize opportunities for public involvement and to minimize the amount of relevant information that is withheld from the public.

Congress should mandate an independent review of the methodology used by the NRC to develop the DBT and the adequacy of the DBT itself, in light of intelligence on known and emerging threats. The views of all other agencies should be seriously considered. An approach similar to that proposed in the House and Senate energy bills, which would require an interagency review of threats and assignments of responsibility for addressing them, would be a good start.

Force-on-Force Tests

A key aspect of a robust security program is force-on-force (FOF) testing. 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

[8] Michael Wallace, President, Constellation Group, Chairman of NEI Security Working Group and Chairman of the Nuclear Sector Coordinating Council, "Achieving Stability in a Post-9/11 Environment," NRC Regulatory Information Conference, Rockville, MD, March 8, 2005.

security orders, that will test the security of each plant site every three years. 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. Congress should consider legislation that would impose strict guidelines on the FOF testing program to ensure that these concerns and others are resolved.

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. NRC's 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, obviously presents the potential for conflicts of interest. While NRC asserts that it is rigorously guarding against the possibility that the tests could be compromised, the public has no choice but to take NRC at its word. In this regard, appearance is everything.

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.

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.

Guard Fatigue

Another critical issue is guard fatigue. The job of security personnel at nuclear plants is a demanding and stressful one. They must be poised to respond to an attack with little or no warning during their entire shift. And if an attack comes, they must respond consistently at the highest level of performance. Strong safeguards must be in place to ensure that security officers get enough rest to do their job effectively. In 2003, after numerous reports that security officers around the country were being compelled by management to work unreasonably long hours, such as six consecutive twelve-hour shifts per week, the NRC imposed an order putting modest restrictions on their work hours. But UCS and other watchdog groups continue to hear complaints that licensees are not fully complying with the order or are exploiting loopholes in it, and that the NRC is not aggressively enforcing the order. If these complaints have merit, this state of affairs needs to be immediately addressed.

Risk-Informed Regulation: Still a Single-Edged Sword

One of the most glaring examples of the NRC's slant toward the interests of licensees can be found in its selective implementation of "risk-informed regulation." This is a process in which safety regulations are reviewed, using probabilistic risk assessment techniques, to evaluate their

impact on radiological risk to the public. Those regulations that are determined not to have a significant impact on reducing risk can then be scrapped.

The NRC has said that risk-informed regulation should be a "double-edged sword" — that is, the process should be used not only to eliminate regulations and reduce regulatory burden, but also to strengthen regulations when gaps in protection are found that have high risk significance. But, as UCS Reactor Safety Engineer David Lochbaum has said, the NRC's "two-edged risk-informed sword" is "razor-sharp on one side, NERF-like on the other."[9] In other words, it is much more effective in reducing regulatory burdens than in imposing new requirements.

When confronted with this criticism, the NRC has offered a counterexample: its revision of regulation 10 C.F.R. 50.44, which concerns the control of combustible gases (such as hydrogen) during accidents to prevent an explosion that could breach containment. However, a look at the specifics of this case demonstrates otherwise.

The NRC's analysis found that most of the requirements for controlling hydrogen generation have little impact on the risk of containment failure. But it also found that there was one case in which the regulations did not adequately limit the risk of containment failure for certain types of plants during station blackouts, in which both off-site and on-site power is lost. Of the plants in this category, nine are pressurized-water reactors with ice-condenser containments, such as Catawba I and II in South Carolina, and four are boiling-water reactors with Mark III containments, such as Perry in Ohio. These plants have significantly smaller and weaker containments than other U.S. plants, and in the event of a hydrogen explosion, studies show that there would be a near certainty of containment failure,[10] resulting in a catastrophic radiological release. For this reason, NRC requires that these plants be provided with hydrogen igniters to burn off hydrogen generated during an accident before it can reach an explosive concentration. However, these igniters require AC power to operate, so in the event of a station blackout, they would not be available, and operators would be helpless to prevent a containment failure.

[9] Presentation by David Lochbaum at the NRC Nuclear Safety Research Conference, October 30, 2002.
[10] U.S. NRC, "Director's Status Report on Generic Activities," April 2005, p. 90.

The NRC revised 10 CFR 50.44 by throwing out all the provisions that it determined were unnecessary. However, it also decided to evaluate whether it would be cost-effective to require that ice-condenser and Mark III plants be equipped with additional backup power supplies to ensure that the igniters would be available during a blackout. After several years of detailed analyses, the NRC decided that this problem could be fixed inexpensively and that the reduction in risk was well worth the cost. This seemed to be a win-win-win situation: the public would win because a serious risk would be mitigated; licensees would win because the fix was quick and not prohibitively expensive, and the NRC would win by being able to show naysayers that it wasn't afraid to impose additional requirements when necessary.

However, four years later, virtually nothing has happened. Boiling-water reactor operators insisted on imposing strict design criteria on replacement power systems that drove up their projected cost until they no longer looked justifiable. And not only has the NRC abandoned plans to fix the problem through a rulemaking, it has even declined to issue a generic letter requiring licensees to make the necessary changes. It is now relying on voluntary commitments, but some licensees may not even follow through with those, claiming that they are too expensive. Meanwhile, people living near those plants remain at an unnecessarily high risk of being victims of a Chernobyl-type accident. If uncorrected, this problem will pose an even greater risk if the Catawba and McGuire ice-condenser plants begin to utilize large quantities of plutonium-bearing MOX fuel, which can increase both the probability and consequences of a severe accident or a successful radiological sabotage attack. The second edge of NRC's risk-informed sword has yet again proved to be a dull blade.

Safety Culture at the NRC

My colleague at UCS, David Lochbaum, who is an expert in safety issues, was not able to be here today. Here I would like to outline his views on the need for an improved safety culture at the NRC.

According to the NRC, a safety culture "*can be characterized by a willingness on the part of licensee staff to raise and document safety issues to resolve risk-significant equipment and*

process deficiencies promptly, adhere to written procedures, conduct effective training, make conservative decisions, and conduct probing self-assessments."

In recent years, the NRC did not allow the Millstone and Davis-Besse reactors to restart until their safety cultures had been restored to acceptable levels. However, independent assessments performed by the General Accounting Office and the NRC Inspector General of the safety culture within NRC conclude it is as bad as, if not worse, than that at Millstone or Davis-Besse.[11] For example, nearly 50 percent of NRC staffers in a recent survey reported feeling unable to raise safety concerns without fear of retaliation and nearly one-third of NRC staffers who had raised safety concerns felt they had suffered harassment and/or intimidation as a result.

These assessments of the NRC safety culture are consistent with reports UCS has received from NRC staffers who have called with accounts of NRC inspectors being instructed by their managers not to find any violations, of NRC managers telling inspectors not to write up safety problems they found at nuclear plants, and of NRC managers ignoring the written objections of the agency's subject matter experts when making decisions about safety. Such behavior is unacceptable and must be corrected.[12]

Thus far, the NRC has failed to do anything to remedy its own safety culture problems. The NRC will not allow a nuclear reactor to operate if it feels the work force labors under a poor safety culture. By the same token, the NRC's own staff must function in a good safety culture if we are to have confidence in its oversight of the entire reactor fleet. The safety culture within the NRC must be monitored and restored to at least the level that the NRC deems minimally acceptable for operating nuclear plants.

---

[11] GAO on NRC: United States General Accounting Office, "Nuclear Regulation: NRC Staff Have Not Fully Accepted Planned Changes," GAO/RCED-00-29, January 2000.
IG on NRC: United States Nuclear Regulatory Commission Inspector General, "Special Evaluation: OIG 2002 Survey of NRC's Safety Culture and Climate,' OIG-03-A-03, December 11, 2002.
Millstone: Presentation by Little Harbor Consultants to Nuclear Regulatory Commission, "Update on LHC Oversight Activities at Millstone," July 22, 1997.
Davis-Besse: Letter from FirstEnergy Nuclear Operating Company to Nuclear Regulatory Commission, "Submittal of the Report Titled 'Safety Culture Evaluation of the Davis-Besse Nuclear Power Station,' dated April 14, 2003," April 23, 2003.

[12] Letter from David Lochbaum, to NRC Chairman Nils Diaz, "Kudos and Mea Culpa on Safety Conscious Work Environment," February 2, 2004.

Summary

The NRC has repeatedly testified since 9/11 that it opposes many of the legislative initiatives proposed in both houses of Congress to strengthen nuclear plant security on the grounds that they are unnecessary. UCS believes that legislative reform is necessary and appropriate to ensure that design basis threats are realistic and conservative; that required resources are made available for protection against beyond-design-basis threats; that security testing is effective and credible; that emergency planning procedures are designed to protect all individuals at risk from a nuclear plant sabotage attack; and that protections against theft of nuclear weapon-usable materials are strengthened, not weakened. We look forward to working with you to ensure that operating nuclear power plants remain as safe and secure as possible.