



P.O. Box 164  
Pismo Beach, CA 93448  
(805) 773-3881  
[www.mothersforpeace.org](http://www.mothersforpeace.org)

**Supporting Document**

**for**

**A Call for Action to Protect the Nation  
against Enemy Attack  
on Nuclear Power Plants and Spent Fuel**

May 2003

prepared for

Mothers for Peace

by

Institute for Resource and Security Studies  
27 Ellsworth Avenue, Cambridge, MA 02139  
Phone: 617-491-5177 Fax: 617-491-6904  
Email: [info@irss-usa.org](mailto:info@irss-usa.org)  
Web: [www.irss-usa.org](http://www.irss-usa.org)

## **Preface**

The Mothers for Peace has initiated a call for action to protect the United States against enemy attack on nuclear power plants and spent fuel. Specific actions by local, state and federal governments, citizens and the nuclear industry are called for. To provide supporting information, the Mothers for Peace commissioned the preparation of this document.

This document was prepared by the Institute for Resource and Security Studies (IRSS), an independent, nonprofit organization based in Cambridge, Massachusetts. IRSS was founded in 1984 to conduct technical and policy analysis and public education, with the objective of promoting international security and sustainable use of natural resources.

The author of this document is Gordon Thompson, the executive director of IRSS and a research professor at Clark University. Dr. Thompson has extensive experience in technical and policy analysis related to the security of nuclear facilities.

**Table of Contents**

1. Introduction
2. Basic information about nuclear power plants and spent fuel
3. NRC regulations for protection of nuclear facilities and spent-fuel shipments
4. The potential for attack
5. Vulnerability of nuclear facilities and spent-fuel shipments
6. Measures for protecting nuclear facilities and spent-fuel shipments
7. Efforts by local and state governments and citizens to obtain protection
8. Policy initiatives that are needed
9. Establishing an independent technical capability
10. References

## **1. Introduction**

"Homeland security, particularly in the context of critical infrastructure and key asset protection, is a shared responsibility that cannot be accomplished by the federal government alone. It requires coordinated action on the part of federal, state, and local governments; the private sector; and concerned citizens across the country."

National Strategy for Physical Protection of Critical  
Infrastructures and Key Assets<sup>1</sup>

US nuclear power plants and their spent fuel are prime targets for attack by foreign or domestic enemies. The nation's 103 commercial nuclear reactors, their associated spent-fuel pools, and the growing number of independent spent-fuel-storage installations (ISFSIs) are large, fixed targets that are, in a military sense, lightly defended. Although massive in their construction, these facilities are not designed to resist attack and have a number of vulnerabilities. Spent nuclear fuel is also vulnerable during transportation. A successful attack on a nuclear power plant, an ISFSI or a spent-fuel shipment could produce a large release of radioactive material, with severe impacts on health, the environment, the economy and society.

As the White House says in the national strategy document quoted above, protection of key assets -- such as nuclear power plants -- requires cooperation by citizens, industry and all levels of government. One could expect, therefore, that the US Nuclear Regulatory Commission (NRC) would welcome the involvement of local and state governments and citizen groups in protecting nuclear power plants and spent fuel. Unfortunately, the NRC's cooperation extends only to the nuclear industry. Before and after the attacks of 11 September 2001, local and state governments and citizen groups have been rebuffed by the NRC when they sought to participate in decision making about protective measures at nuclear facilities. To help correct this situation, the Mothers for Peace has issued a Call for Action. The Call sets forth specific actions whereby all levels of government, together with citizens and industry, can cooperate to protect the nation against enemy attack on nuclear power plants and spent fuel. This document provides information that supports the Call.

Homeland security poses a challenge to our social institutions. We must make clear-headed assessments of the risk of attack and the options available for protecting potential targets. These assessments must be informed by the best possible technical analysis, but detailed analysis may be inappropriate for open publication because it could assist attackers. Difficult decisions must be made about the general level of investment in homeland security, and about the allocation of that investment across potential targets. The probability of a highly-damaging attack must be minimized without undermining civil

---

<sup>1</sup> White House, 2003, page vii.

liberties or the economy. Our homeland-security strategy and our national-security strategy must be complementary.

For many years, US national-security policy has assigned a higher priority to offensive actions worldwide than to defensive actions within the homeland.<sup>2</sup> However, in the contemporary era of asymmetric warfare, this policy can be dangerous. If our key assets -- such as nuclear power plants -- are poorly defended, we may feel compelled to use military force aggressively around the world, in order to pre-empt or punish attackers.<sup>3</sup> Such action poses the risk of arousing hostility and promoting anarchy, leading to new attacks on our homeland. The potential exists for an escalating spiral of violence. Moreover, if we reduce civil liberties out of fear that key assets are vulnerable, we run the risk of increasing the number of domestic enemies. Thus, decisions about the protection of key assets and infrastructure are of the highest national importance.

Fortunately, measures are available whereby the protection of US nuclear facilities can be improved. Implementation of a suite of measures could substantially reduce the probability that an attack on a nuclear power plant or spent fuel would result in a large release of radioactive material. These measures, appropriately advertised, would deter attackers. Potential attackers have finite resources, and will therefore avoid targets where it is likely that an attack would fail. Successful deterrence of attacks would allow us to preserve our civil liberties and be cautious in using our military capabilities offensively. Moreover, protective measures could prevent or substantially reduce offsite harm if deterrence failed and an attack occurred.

The preceding paragraphs give a sense of the importance of protecting nuclear facilities, and the complexity of some of the issues involved. Faced with such complexity, people might be tempted to leave this problem in the hands of the NRC and the nuclear industry. However, these entities cannot be relied upon to provide the protection that is needed. Citizens and public officials at all levels of government must, therefore, become involved. This document is intended to provide information to support their involvement. Major technical and policy issues are briefly reviewed here, and documents are cited that address these issues in greater depth.

As mentioned above, detailed analysis on the risk of attack and the effectiveness of protective measures may be inappropriate for open publication. Yet, repeated experience shows that secrecy breeds complacency and bureaucratic defensiveness, and allows special interests to unduly influence decision making. These behaviors are currently evident in the arena of nuclear-facility security. The NRC conducts secret discussions with the nuclear industry but excludes other knowledgeable stakeholders. Industry

---

<sup>2</sup> The current US national-security strategy (White House, 2002) continues the longstanding emphasis on offensive capabilities, and adds a new emphasis on pre-emptive attack.

<sup>3</sup> The interplay between homeland-security measures and offensive actions worldwide has been discussed by many observers, including a high-level task force convened by the Council on Foreign Relations (Hart et al, 2002).

exploits its special access in order to resist measures for improved protection of nuclear facilities, and the NRC rarely challenges the industry. Thus, there is a need for an independent capability to review threat assessments, vulnerability assessments and plans for protective measures. The Call for Action asks state governments to sponsor such a capability. Section 9 of this document discusses this matter further.

## **2. Basic information about nuclear power plants and spent fuel**

At a nuclear power plant, fission energy is released in a nuclear reactor. There are 103 commercial reactors operating in the USA at 65 sites in 31 states.<sup>4</sup> Of these 103 reactors, 69 are pressurized-water reactors (PWRs), 9 with ice-condenser containments and 60 with dry containments. The remaining 34 reactors are boiling-water reactors (BWRs), 22 with Mark I containments, 8 with Mark II containments and 4 with Mark III containments. In addition there are 27 previously-operating commercial reactors in various stages of storage or decommissioning. As of December 2000, all but 2 of the 103 operating reactors had been in service for at least 9 years, and 55 reactors had been in service for at least 19 years.<sup>5</sup> Thus, the reactor fleet is aging. The nominal duration of a reactor operating license is 40 years.

Four of the 103 operating reactors have design features intended to resist aircraft impact. The Limerick Unit 1, Limerick Unit 2 and Seabrook reactors were designed to withstand the impact of an aircraft weighing 6 tonnes, while the Three Mile Island Unit 1 reactor was designed to withstand the impact of an aircraft weighing 90 tonnes. No other US reactor was designed to withstand aircraft impact.<sup>6</sup>

### *Wet and Dry Storage of Spent Fuel*

The core of a commercial nuclear reactor consists of several hundred fuel assemblies.<sup>7</sup> Each fuel assembly contains thousands of cylindrical, uranium-oxide pellets stacked inside long, thin-walled tubes made of zirconium alloy. These tubes are often described as the "cladding" of the fuel. After several years of use inside an operating reactor, a fuel assembly becomes "spent" in the sense that it is no longer suitable for generating fission power. Then, the fuel is discharged from the reactor and placed in a water-filled pool adjacent to the reactor but outside the reactor containment. This fuel, although spent, contains numerous radioactive isotopes whose decay generates ionizing radiation and heat. Fuel assemblies in the reactor core or the spent-fuel pool contain almost all of the radioactive inventory at a nuclear power plant.

---

<sup>4</sup> In addition, Browns Ferry Unit 1, a BWR with a Mark I containment, is nominally operational. However, it is defueled and not in service.

<sup>5</sup> Data from the NRC website ([www.nrc.gov](http://www.nrc.gov)), 24 April 2002.

<sup>6</sup> Markey, 2002, page 73.

<sup>7</sup> The number of fuel assemblies in a reactor core ranges from 121 (in some PWRs) to 764 (in some BWRs).

After a period of storage in a pool, the thermal power produced by a fuel assembly declines to a level such that the assembly can be transferred to a dry-storage ISFSI. The present US approach to ISFSI design is to store spent fuel inside helium-filled, passively-cooled containers that are placed on concrete pads in the open air. Current practice is to allow a minimum cooling period of 5 years before transfer to dry storage. However, this cooling period reflects an economic and safety tradeoff rather than a fundamental physical limit. Fuel cooled for a shorter period than 5 years could be transferred to dry storage, but in that case fewer assemblies could be placed in each dry-storage container. Alternatively, older and younger spent fuel (counting age from the date of discharge from the reactor) could be co-located in a dry-storage container. The major physical limit to placement of spent fuel in dry storage is the maximum temperature of the cladding, which the NRC typically sets at 400 degrees C. This temperature limit constrains the allowable heat output of the fuel, which in turn constrains the cooling period.

#### *Development of ISFSIs*

There are now 20 ISFSIs in the USA, of which 15 are at sites where commercial reactors are in operation.<sup>8</sup> More ISFSIs will be needed, because the spent-fuel pools at operating reactors are filling up. Analysis done at MIT shows that, by 2005, almost two-thirds of reactor licensees will face the need to acquire onsite dry-storage capacity, even if shipment of spent fuel away from the reactor sites begins in 2005.<sup>9</sup> NAC International, a consulting firm and vendor of dry-storage technology, reaches similar conclusions. NAC estimates that, at the end of 2000, about 6 percent of the US inventory of commercial spent fuel was stored in ISFSIs at reactor sites, whereas about 30 percent of the inventory will be stored in ISFSIs by 2010.<sup>10</sup> New ISFSIs will generally be at reactor sites, although some might be at new sites. Currently, only one proposed ISFSI at a new site -- Skull Valley, Utah -- is a plausible candidate for operation by 2010. However, in March 2003 an NRC licensing board denied a construction and operating license for the Skull Valley ISFSI, and the future of this project is uncertain.

#### *Transportation of Spent Fuel*

At present, almost all US spent fuel is stored at reactor sites. If spent fuel were shipped away from a site, this would be done by placing the fuel inside a spent-fuel-transport cask that would be carried on a truck, railcar or ship. The fuel could have three possible destinations. First, fuel could be transported to another reactor site, which is now being done by one licensee. Progress Energy transports fuel from its Brunswick and Robinson

---

<sup>8</sup> Data from the NRC website ([www.nrc.gov](http://www.nrc.gov)), 24 April 2002.

<sup>9</sup> Macfarlane, 2001a.

<sup>10</sup> NAC, 2001. NAC estimates that the end-2000 US inventory of spent fuel was 42,900 tonnes, of which 2,430 tonnes was in ISFSIs. Also, NAC estimates that the 2010 US inventory will be 64,300 tonnes, of which 19,450 tonnes will be in ISFSIs.

reactors to its Harris site, but has signaled its intention to phase out these transfers.<sup>11</sup> Second, fuel could be transported to an ISFSI at an away-from-reactor site, such as Skull Valley. Third, fuel could be transported to a future repository at Yucca Mountain, Nevada. At Yucca Mountain, the fuel would be emplaced in underground tunnels. Under some scenarios for the operation of Yucca Mountain, emplacement of fuel would be preceded by a period of interim storage at the surface.

### *Yucca Mountain*

The Yucca Mountain repository project is the federal government's proposed long-term solution to the problem of spent-fuel management. If this repository opens, there will be numerous shipments of spent fuel to Yucca Mountain. However, the Yucca Mountain project will not eliminate the need for additional ISFSI capacity, for reasons summarized in the following three paragraphs.

First, the Yucca Mountain repository may never open. This project is politically driven, lacks a scientific basis, and is going forward only because previously-specified technical criteria for a repository have been abandoned.<sup>12</sup> These deficiencies add weight to the determined opposition to this project by the state of Nevada and other entities. Their opposition reflects concerns about potential leakage from the repository, the risk of transporting fuel to Yucca Mountain, and the unfair political process whereby this site was selected.

Second, decades will pass before fuel can be emplaced in a repository at Yucca Mountain. The US Department of Energy (DOE) claims that it can open the repository in 2010, but the US General Accounting Office has determined that several factors, including budget limitations, could extend this date to 2015 or later.<sup>13</sup> DOE envisions that, after the repository is opened, emplacement of fuel will occur over a period of at least 24 years and potentially 50 years.<sup>14</sup> This vision may prove to be optimistic.

Third, under present federal law the Yucca Mountain repository will hold no more than 63,000 tonnes of commercial spent fuel.<sup>15</sup> Yet, the cumulative amount of commercial spent fuel to be generated during the lifetimes of the 103 currently-licensed reactors is

---

<sup>11</sup> The Harris site features one reactor and four spent-fuel pools, and thus has more pool-storage capacity than other reactor sites. Spent fuel that is shipped to Harris is placed in a pool, and there is no current plan to build an ISFSI at Harris.

<sup>12</sup> Ewing and Macfarlane, 2002.

<sup>13</sup> Jones, 2002b.

<sup>14</sup> DOE, 2002. DOE contemplates the construction of a surface facility for interim storage of spent fuel at Yucca Mountain, especially if emplacement of fuel occurs over a period of 50 years. However, given the cost of this surface facility, a more likely alternative is that fuel would remain in ISFSIs until it could be emplaced in the repository.

<sup>15</sup> DOE, 2002. The Nuclear Waste Policy Act limits the total amount of waste that can be placed in a first repository to 70,000 tonnes until a second repository is in operation. DOE plans to use 63,000 tonnes of this capacity for commercial spent fuel. DOE has studied the possible expansion of Yucca Mountain's capacity to include 105,000 tonnes of commercial spent fuel together with other wastes.

likely to exceed 80,000 tonnes.<sup>16</sup> Reactor licensees have shown strong interest in obtaining license extensions which, if granted, would lead to the production of a substantial additional amount of spent fuel.

### **3. NRC regulations for protection of nuclear facilities and spent-fuel shipments**

The NRC's basic policy on protecting nuclear facilities from attack is laid down in the regulation 10 CFR 50.13. This regulation was promulgated in September 1967 by the US Atomic Energy Commission (AEC) -- which preceded the NRC -- and was upheld by the US Court of Appeals in August 1968. It states:<sup>17</sup>

"An applicant for a license to construct and operate a production or utilization facility, or for an amendment to such license, is not required to provide for design features or other measures for the specific purpose of protection against the effects of (a) attacks and destructive acts, including sabotage, directed against the facility by an enemy of the United States, whether a foreign government or other person, or (b) use or deployment of weapons incident to US defense activities."

The AEC was motivated to introduce this regulation by the intervention of a citizen -- Paul Siegel -- in the construction-license proceeding for the Turkey Point nuclear power plants in Florida. Mr. Siegel argued that these plants might be attacked from Cuba. The AEC pre-empted any consideration of this issue during the license proceeding by initiating the rulemaking process that led to 10 CFR 50.13.

Pursuant to this regulation, the NRC's licensees are not required to design or operate nuclear facilities to resist enemy attack. However, events have forced the NRC to progressively modify this position, so as to require greater protection against acts of malice or insanity. A series of events, including the 1993 bombing of the World Trade Center in New York, eventually forced the NRC to introduce, in 1994, regulations requiring licensees to defend nuclear power plants against vehicle bombs. The terrorist events of 11 September 2001 have forced the NRC to require additional measures. Nevertheless, present NRC regulations require only a light defense of nuclear facilities.

#### *NRC Regulations for Site Security*

Present NRC regulations for the defense of nuclear facilities are focused primarily on site security, which the NRC discusses under the heading "physical protection". As described in Section 6, below, site security is one of four types of measure that, taken together, could provide a defense in depth against acts of malice or insanity. The other

---

<sup>16</sup> Macfarlane, 2001a.

<sup>17</sup> Federal Register, Vol. 32, No. 186, 26 September 1967, page 13445.

three types of measure are, with some limited exceptions, ignored in present NRC requirements for facility defense.<sup>18</sup>

At a nuclear power plant or an ISFSI, the NRC requires the licensee to implement a set of physical protection measures. According to the NRC, these measures provide defense in depth by taking effect within defined areas with increasing levels of security. Within the outermost physical protection area, known as the Exclusion Area, the licensee is expected to control the area but is not required to employ fences and guard posts for this purpose. Within the Exclusion area is a Protected Area encompassed by physical barriers including one or more fences, together with gates and barriers at points of entry. Authorization for unescorted access within the Protected Area is based on background and behavioral checks. Within the Protected Area are Vital Areas and Material Access Areas that are protected by additional barriers and alarms; unescorted access to these locations requires additional authorization.

Associated with the physical protection areas are measures for detection and assessment of an intrusion, and for armed response to an intrusion. Measures for intrusion detection include guards and instruments whose role is to detect a potential intrusion and notify the site security force. Then, security personnel seek additional information through means such as direct observation and closed-circuit TV cameras, to assess the nature of the intrusion. If judged appropriate, an armed response to the intrusion is then mounted by the site security force, potentially backed up by local law enforcement agencies and the FBI.

### *The Design Basis Threat*

The design of physical protection areas and their associated barriers, together with the design of measures for intrusion detection, intrusion assessment and armed response, is required to accommodate a "design basis threat" (DBT) specified by the NRC. At a nuclear power plant, the dominant sources of hazard are the reactor and the spent-fuel pool(s). In theory, both of these items receive the same level of protection, but in practice the reactor has been the main focus of attention. The DBT for an ISFSI is less demanding than that for a nuclear power plant.

In April 2003 the DBT for a nuclear power plant was revised, but the NRC has announced that the features of the revised DBT will not be published. The previously-applicable DBT had the following features:<sup>19</sup>

---

<sup>18</sup> For information about the NRC's present regulations and requirements for nuclear-facility defense, see: the NRC website ([www.nrc.gov](http://www.nrc.gov)), accessed by IRSS on 23 May 2003; Markey, 2002; Meserve, 2002; Meserve, 2003; and NRC, 2002.

<sup>19</sup> 10 CFR 73.1, Purpose and Scope, from the NRC web site ([www.nrc.gov](http://www.nrc.gov)), accessed on 2 September 2002.

"(i) A determined violent external assault, attack by stealth, or deceptive actions, of several persons with the following attributes, assistance and equipment: (A) Well-trained (including military training and skills) and dedicated individuals, (B) inside assistance which may include a knowledgeable individual who attempts to participate in a passive role (e.g., provide information), an active role (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack), or both, (C) suitable weapons, up to and including hand-held automatic weapons, equipped with silencers and having effective long range accuracy, (D) hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container integrity or features of the safeguards system, and (E) a four-wheel drive land vehicle used for transporting personnel and their hand-carried equipment to the proximity of vital areas, and

(ii) An internal threat of an insider, including an employee (in any position), and

(iii) A four-wheel drive land vehicle bomb."

For an ISFSI, the DBT was the same as for a nuclear power plant except that it did not include the use of a four-wheel-drive land vehicle, either for transport of personnel and equipment or for use as a vehicle bomb. This was true whether the ISFSI was at a new site or a reactor site. Thus, an ISFSI at a reactor site would be less protected than the reactor(s) and spent-fuel pool(s) at that site. At a reactor site or a new site, an ISFSI would be vulnerable to attack by a vehicle bomb.

#### *Evolution of the DBT*

After the events of 11 September 2001, the NRC concluded that its requirements for nuclear facility security were inadequate. Accordingly, the NRC issued an order to licensees of operating plants in February 2002, and similar orders to licensees of decommissioning plants in May 2002 and reactor-site ISFSI licensees in October 2002, requiring "certain compensatory measures", also described as "prudent, interim measures", whose purpose was to "provide the Commission with reasonable assurance that the public health and safety and common defense and security continue to be adequately protected in the current generalized high-level threat environment".<sup>20</sup> The additional measures required by these orders were not publicly disclosed, but the NRC Chairman has stated that they included:<sup>21</sup>

---

<sup>20</sup> The quoted language is from page 2 of the NRC's order of 25 February 2002 to all operating power reactor licensees. Almost-identical language appears in the NRC's orders of 23 May 2002 to all decommissioning power reactor licensees and 16 October 2002 to all ISFSI licensees who also hold 10 CFR 50 licenses.

<sup>21</sup> Meserve, 2002.

- (i) increased patrols;
- (ii) augmented security forces and capabilities;
- (iii) additional security posts;
- (iv) vehicle checks at greater stand-off distances;
- (v) enhanced coordination with law enforcement and military authorities;
- (vi) additional restrictions on unescorted access authorizations;
- (vii) plans to respond to plant damage from explosions or fires; and
- (viii) assured presence of Emergency Plan staff and resources.

In addition to requiring these additional security measures, the NRC established a Threat Advisory System that warns of a possible attack on a nuclear facility. This system uses five color-coded threat conditions ranging from green (low risk of attack) to red (severe risk of attack). These threat conditions conform with those used by the Department of Homeland Security.

The NRC has described its new, revised DBT for nuclear power plants as follows:<sup>22</sup>

"The Order that imposes revisions to the Design Basis Threat requires power plants to implement additional protective actions to protect against sabotage by terrorists and other adversaries. The details of the design basis threat are safeguards information pursuant to Section 147 of the Atomic Energy Act and will not be released to the public. This Order builds on the changes made by the Commission's February 25, 2002 Order. The Commission believes that this DBT represents the largest reasonable threat against which a regulated private security force should be expected to defend under existing law. It was arrived at after extensive deliberation and interaction with cleared stakeholders from other Federal agencies, State governments and industry."

*Inferred Characteristics of the New DBT*

Although the new DBT for nuclear power plants will not be published, its general characteristics can be inferred with reasonable confidence. Four major considerations support such an inference. First, the new DBT must be consistent with 10 CFR 50.13. Second, the DBT will not exceed the capabilities of a "regulated private security force". Third, there is a well-documented history over the past two decades, showing vigorous resistance by the nuclear industry to measures that enhance site security, and a reluctance by the NRC to contest that resistance.<sup>23</sup> Fourth, available information shows no marked change in prevailing practices of site security.<sup>24</sup>

---

<sup>22</sup> NRC Press Release No. 03-053, 29 April 2003.

<sup>23</sup> Hirsch et al, 2003.

<sup>24</sup> POGO, 2002; Brian, 2003.

Thus, it can be inferred that the new DBT remains focussed on a ground assault by a comparatively small group of lightly-armed attackers. The most destructive instrument included in the DBT is probably a vehicle bomb. The new DBT probably does not allow for aerial or multimodal attack by a commando-type force. It probably does not allow for antitank missiles or lethal chemical weapons. There is probably no provision for an attack using a commercial or general-aviation aircraft, with or without a load of fuel or explosive. There is no provision for attack using a nuclear weapon. The insider threat probably does not include carefully-planned, sophisticated interventions by key employees. Also, the new DBT does not apply to ISFSIs, so it can be assumed that ISFSIs continue to receive a lesser degree of protection than nuclear power plants.

#### *Protection of Spent-Fuel Shipments*

Requirements for physical protection of spent-fuel shipments are laid down by the NRC in the regulation 10 CFR 73.37.<sup>25</sup> The required protection consists of armed escorts who make radio contact with a communications center at least every two hours.<sup>26</sup> Two escorts are required when the shipment is in a heavily-populated area, but only one escort is required when the shipment is not in such an area. 10 CFR 73.37 does not specify the robustness of the container in which spent fuel is shipped. Other regulations, that focus on safety issues such as the possibility of a collision or fire during shipment, do address container robustness.

#### **4. The potential for attack**

The NRC's new DBT for nuclear power plants reflects the agency's judgement about the probabilities of attacks at various levels of severity. As inferred above, the DBT remains focussed on a ground assault by a comparatively small group of lightly-armed attackers. Requirements for physical protection of spent-fuel shipments assume a lesser threat. Presumably, the NRC has concluded that attacks more severe than the assumed threats are unlikely to occur. For example, the NRC does not require protection against an attack by an explosive-laden, general-aviation aircraft, presumably on the basis that this is an unlikely event.

One hopes that the NRC's judgment is accurate. However, there is reason to fear that the NRC has not properly understood the present global threat environment, and has therefore under-estimated the potential for highly-damaging attacks. A full discussion of the global threat environment is beyond the scope of this paper, but the considerations outlined in the following paragraphs provide grounds for concern.

The United States has highly-capable military forces, as illustrated by our recent invasion of Iraq. These forces provide us with an unparalleled ability to coerce foreign nations.

---

<sup>25</sup> 10 CFR 73.37, Requirements for physical protection of irradiated reactor fuel in transit, from the NRC website ([www.nrc.gov](http://www.nrc.gov)), accessed 20 May 2003.

<sup>26</sup> During sea shipment of spent fuel, radio contact is required only while the vessel is in port.

However, there are two major ways in which our military capability may be ineffective or even counterproductive in the context of nuclear-facility security. First, our military dominance will drive enemies to an asymmetric response, and nuclear facilities are potential targets of such a response. Second, our use of military force around the world may increase the number and level of commitment of foreign enemies and their sympathizers.<sup>27</sup> Thus, the potential exists for an escalating spiral of violence in which our nuclear facilities become weapons to be used against us.

Small or medium-sized nations with which we might be in conflict will recognize that a direct military confrontation with us is probably a losing proposition. Thus, they will seek options for asymmetric response, with the objective of deterring or punishing our attack. One such option is a small nuclear arsenal.<sup>28</sup> Another option is to develop the capacity to attack our homeland by turning our own technologies against us. Nuclear facilities are prime targets for such attack because they are lightly-defended structures that could, if successfully attacked, cause us great harm. Also, civilian nuclear facilities may be targeted because they symbolize our superiority in nuclear weapons, which we flaunt while seeking to deny nuclear weapons to other nations.<sup>29</sup>

Sub-national groups that use violence for political ends will inevitably opt for asymmetric warfare, because they lack any military capacity. Moreover, since they lack territory that we can counter-attack, such groups may not hesitate to provoke us through a damaging attack on our homeland. Indeed, their purpose might be to provoke us into aggressive actions that will ultimately serve their political ends. Thus, sub-national enemy groups will inevitably contemplate attacking our nuclear facilities. Whether or not they proceed with such an attack will depend on their assessment of the probability of success.

There is reason for concern that our military actions around the world will increase the number and level of commitment of foreign enemies. Our invasion of Iraq was widely opposed and may, on balance, have increased the risk of attack on US assets.<sup>30</sup> The full implications of this invasion for our security will not be apparent for some years. Also, it is important to note that the Iraq invasion was one of a sequence of foreign interventions. In recent years we have attacked Serbia (1999), Afghanistan (2001) and Iraq (2003), and government officials are now signaling an interest in attacking Iran. Whatever the merits of these attacks might be, their cumulative effects will undoubtedly include a legacy of grievance. As a nation of immigrants and a destination for millions of travellers, we should be concerned about the possibility of a growing number of citizens and visitors who sympathize with foreign enemies. Moreover, if we curb civil liberties

---

<sup>27</sup> A recent survey of public opinion around the world shows that the US invasion of Iraq "has widened the rift between Americans and Western Europeans, further inflamed the Muslim world, softened support for the war on terrorism, and significantly weakened global public support for the pillars of the post-World War II era -- the UN and the North Atlantic Alliance (Pew, 2003, Introduction and Summary, page 1).

<sup>28</sup> North Korea argues that its emerging nuclear arsenal is needed to deter attack by the United States.

<sup>29</sup> Scarry, 2002.

<sup>30</sup> Pew, 2003.

out of fear of such sympathizers, we risk feeding the growth of domestic right-wing groups that have demonstrated a willingness to perform destructive acts.<sup>31</sup>

Weighing all the factors that affect our security is a difficult exercise, calling for mature judgement informed by clear-headed assessments. Regrettably, decisions about homeland security and national security are not always made in this way. Statements made by the leadership of the NRC do not create confidence that decision-making about the new DBT for nuclear power plants was well informed.<sup>32</sup>

The main determinant of the risk of attack on our nuclear facilities is the number and type of people who are motivated to conduct an attack. If the number of such people grows, especially if it includes people with a technical education or military experience, then the risk of attack will grow. Obtaining instruments of attack would not be a major constraint. For example, about 220,000 general-aviation aircraft are in use in the United States, each of which could become an explosive-laden missile guided by a suicidal pilot.<sup>33</sup> Among the possible instruments of attack, we cannot exclude a small nuclear weapon.<sup>34</sup> This instrument, although difficult to obtain, would be attractive to attackers because its radioactive fallout could be hugely amplified by the radioactive release from the targeted facility.

## **5. Vulnerability of nuclear facilities and spent-fuel shipments**

It is not appropriate to publish a detailed discussion of scenarios whereby a nuclear power plant, an ISFSI or a spent-fuel-transport cask might be successfully attacked. However, it must be assumed that attackers are technically sophisticated and possess considerable knowledge about individual nuclear facilities. For decades, engineering drawings, photographs and technical analyses have been openly available for every civilian nuclear facility in the USA. This material is archived at many locations around the world. Thus, a public discussion, in general terms, of potential modes and instruments of attack will not assist attackers. Indeed, such a discussion is needed to ensure that appropriate defensive actions are taken.<sup>35</sup>

### *Safety Systems and their Vulnerability*

The safe operation of a US commercial reactor or a spent-fuel pool depends upon the fuel in the reactor or the pool being immersed in water. Moreover, that water must be

---

<sup>31</sup> Office of Homeland Security, 2002, page 10.

<sup>32</sup> The transcript (NRC, 2003) of a March 2003 meeting of the NRC Commissioners calls into question their professionalism and objectivity.

<sup>33</sup> For a review of potential instruments of attack, see: Thompson, 2003.

<sup>34</sup> A high-level group advising the US government has stated (Baker, Cutler et al, 2001, page 1 of Executive Summary): "The most urgent unmet national security threat to the United States today is the danger that weapons of mass destruction or weapons-usable material in Russia could be stolen and sold to terrorists or hostile nation states and used against American troops abroad or citizens at home."

<sup>35</sup> For a more detailed discussion of nuclear-facility vulnerability, see: Thompson, 2003.

continually cooled to remove fission heat or radioactive decay heat generated in the fuel. A variety of systems are used to ensure that water is available and is cooled, and that other safety-related functions -- such as shutdown of the fission reaction when needed -- are performed. Some of the relevant systems -- such as the electrical switchyard -- are highly vulnerable to attack. Other systems are located inside reinforced-concrete structures -- such as the reactor auxiliary building -- that provide some degree of protection against attack. The reactor itself is inside a containment structure. At some plants, but not all, the reactor containment is a concrete structure that is highly reinforced and comparatively robust. Spent-fuel pools have thick concrete walls but are typically covered by lightweight structures.

#### *Attack through Brute Force or Indirectly?*

A group of attackers equipped with highly-destructive instruments could take a brute-force approach to attacking a reactor or a spent-fuel pool. Such an approach would aim to directly breach the reactor containment and primary cooling circuit, or to breach the wall or floor of a spent-fuel pool. Alternatively, the attacking group could take an indirect approach, and many such approaches will readily suggest themselves to technically-informed attackers. Insiders, or outsiders who have taken over the plant, could obtain a release of radioactive material without necessarily employing destructive instruments. Some attack scenarios will involve the disabling of plant personnel, which could be accomplished by armed attack, use of lethal chemical weapons, or radioactive contamination of the site by an initial release of radioactive material.

#### *Vulnerability of ISFSIs and Transport Casks*

Dry-storage ISFSIs and spent-fuel-transport casks differ from reactors and spent-fuel pools in that their operation is entirely passive. Thus, each dry-storage container in an ISFSI or each transport cask must be attacked directly. To obtain a release of radioactive material, the wall of the fuel container must be penetrated from the outside, or the container must be heated by an external fire to such an extent that the containment envelope fails. The attack could also exploit stored chemical energy in the zirconium cladding of the spent fuel. Combustion of this cladding in air, if initiated, would generate heat that could liberate radioactive material from the fuel to the outside environment. A knowledgeable attacker could combine penetration of the fuel container with the initiation of combustion.

#### *Requirements for a Vulnerability Study*

Every US commercial reactor has been subjected to a probabilistic risk assessment (PRA) or equivalent study.<sup>36</sup> This analysis examined the reactor's potential to experience accidents due to human error, equipment failure or natural forces (e.g., earthquake), but did not consider acts of malice or insanity. No spent-fuel pool or ISFSI has been

---

<sup>36</sup> The state of the art for reactor PRAs is illustrated by: NRC, 1990.

subjected to a PRA-type study or a study of its vulnerability to acts of malice or insanity. Indeed, there has never been a comprehensive study of the vulnerability of any US nuclear facility to acts of malice or insanity. Spurred by the attacks on the World Trade Center and Pentagon in September 2001, the NRC has sponsored some secret studies on nuclear-facility vulnerability. However, available information shows that these studies are narrow in scope and will provide limited guidance regarding the overall vulnerability of nuclear facilities.<sup>37</sup>

A comprehensive study of a facility's vulnerability would begin by identifying a range of potential attacks on the facility. The probability of each potential attack would be qualitatively estimated, with consideration of the factors (e.g., international events, changing availability of instruments of attack) that could alter the probability over time. Site-specific factors affecting the feasibility and probability of attack scenarios include local terrain and the proximity of coastlines, airports, population centers and national symbols. A variety of modes and instruments of attack would be considered.

After identifying a range of potential attacks, a comprehensive study would examine the vulnerability of the subject facility to those attacks. This could be done by adapting and extending known techniques of PRA, with an emphasis on the logical structure of PRA rather than the numerical probabilities of events. The analysis would consider the potential for interactions among facilities at a site. For example, a potentially important interaction could be the prevention of personnel access at one facility (e.g., a spent-fuel pool) due to a release of radioactive material at another facility (e.g., a reactor). Attention would be given to the potential for "cascading" scenarios in which attacks at some parts of a nuclear-power-plant site (e.g., control room, switchyard, diesel generators) lead to releases from reactors and/or spent fuel pools that were not directly attacked.

#### *Working with Partial or Misleading Information*

In the absence of any comprehensive study of vulnerability, one is obliged to rely upon partial information. Also, one must contend with misleading information disseminated by the nuclear industry. An egregious example is a paper in *Science*, a journal that is usually sound.<sup>38</sup> Two points illustrate the low scientific quality of this paper. First, the paper cites an experiment performed at Sandia National Laboratories as proof that an aircraft cannot penetrate the concrete wall of a reactor containment. In response, Sandia officials have stated that the test has no relevance to the structural behavior of a containment wall, a fact that is readily evident from the nature of the test.<sup>39</sup> Second, the paper states, in

---

<sup>37</sup> The NRC's Office of Research Programs has stated (NRC, 2003, page 11): "During 2003 Research will complete the realistic engineering assessments of the vulnerability of nuclear power reactors to aircraft attack and the vulnerability of spent fuel pools to explosive attacks. Two pilot plant assessments are underway to assess the threats and identify any additional potential mitigation options." Although potentially useful, these assessments will yield only a fraction of the information that would be contained in a comprehensive assessment of vulnerability.

<sup>38</sup> Chapin et al, 2002.

<sup>39</sup> Jones, 2002a.

connection with the vulnerability of spent-fuel shipping casks, that "there is virtually nothing one could do to these shipping casks that would cause a significant public hazard".<sup>40</sup> A report prepared by Sandia for the NRC is cited in support of this statement.<sup>41</sup> Yet, examination of the Sandia report reveals that it considers only the effects on a shipping cask of impact and fire pursuant to a truck or train accident. The Sandia report does not address the effects of, for example, attack by an anti-tank missile, a vehicle bomb, or a manually-placed charge.

### *Vulnerability of Spent-Fuel Pools*

The vulnerability of spent-fuel pools deserves special mention for two reasons. First, each pool now contains an amount of long-lived radioactive material that is substantially larger than the amount in a reactor core. Second, loss of water from a pool will cause some or all of the fuel in the pool to self-ignite and burn, releasing a large amount of radioactive material to the atmosphere.<sup>42</sup> The potential for a fire exists because the pools have been equipped with high-density racks. In the 1970s, the spent-fuel pools of US nuclear power plants were typically equipped with low-density, open-frame racks. If water were partially or totally lost from such a pool, air or steam could circulate freely throughout the racks, providing convective cooling to the spent fuel. By contrast, the high-density racks that are used today have a closed structure. To suppress criticality, each fuel assembly is surrounded by solid, neutron-absorbing panels, and there is little or no gap between the panels of adjacent cells. In the absence of water, this configuration allows only one mode of circulation of air and steam around a fuel assembly -- vertically upward within the confines of the neutron-absorbing panels.

If water is totally lost from a high-density pool, air will pass downward through available gaps such as the gap between the pool wall and the outer faces of the racks, will travel horizontally across the base of the pool, will enter each rack cell through a hole in its base, and will rise upward within the cell, providing cooling to the spent fuel assembly in that cell. If the fuel has been discharged from the reactor comparatively recently, the flow of air may be insufficient to remove all of the fuel's decay heat. In that case, the temperature of the fuel cladding may rise to the point where a self-sustaining, exothermic oxidation reaction with air will begin. In simple terms, the fuel cladding -- which is made of zirconium alloy -- will begin to burn. The zirconium-alloy cladding can also enter into a self-sustaining, exothermic oxidation reaction with steam. Other exothermic oxidation reactions can also occur. For simplicity, the occurrence of one or more of the possible reactions can be referred to as a pool fire.

---

<sup>40</sup> Chapin et al, 2002, page 1997.

<sup>41</sup> Sprung et al, 2000.

<sup>42</sup> The NRC has published a variety of technical documents that address spent-fuel-pool fires. The most recent of these documents is: Collins et al, 2000. For more recent analyses of spent-fuel-pool fires, see: Alvarez et al, 2003; Thompson, 2003; and Thompson, 2002. The NRC Staff stated in March 2003 (NRC, 2003, page 10) that it has completed an "integral analysis of a spent fuel pool accident scenario", but this analysis has not been published.

In many scenarios for loss of water from a pool, the flow of air that is described in the preceding paragraph will be blocked. For example, a falling object (e.g., a fuel-transfer cask) might distort rack structures, thereby blocking air flow. An attack might cause debris (e.g., from the roof of the fuel handling building) to fall into the pool and block air flow. The presence of residual water in the bottom of the pool would also block air flow. In most scenarios for loss of water, residual water will be present for significant periods of time. Falling debris from burning fuel assemblies could block air flow to nearby fuel assemblies that have not yet ignited. Blockage of air flow, for whatever reason, will lead to ignition of fuel that has been discharged from a reactor for long periods -- potentially 10 years or longer.

## **6. Measures for protecting nuclear facilities and spent-fuel shipments**

Four types of measure, taken together, could provide a comprehensive, defense-in-depth strategy against acts of malice or insanity at a nuclear facility. The four types of measure, which are described in the following paragraphs, are in the categories: (i) site security; (ii) facility robustness; (iii) damage control; and (iv) emergency response planning. The degree of protection provided by these measures would be greatest if they were integrated into the design of a facility before its construction. However, a comprehensive set of measures could provide significant protection at existing facilities.

### *Site Security*

Site-security measures are those that reduce the potential for implementation of destructive acts of malice or insanity at a nuclear site. Two types of measure fall into this category. Measures of the first type would be implemented at offsite locations, and the implementing agencies might have no direct connection with the site. Airline or airport security measures are examples of measures in this category. Measures of the second type would be implemented at or near the site. Implementing agencies would include the licensee, the NRC and, potentially, other entities (e.g., National Guard, Coast Guard). The physical protection measures now required by the NRC, as discussed in Section 3 of this report, are examples of site-security measures of the second type. More stringent measures could be introduced, such as:

- (i) establishment of a mandatory aircraft-exclusion boundary around the site;
- (ii) deployment of an approaching-aircraft detection system that triggers a sitewide alert when the exclusion boundary is crossed;
- (iii) deployment of automated missiles to destroy aircraft closing on the site;
- (iv) expansion of the DBT, beyond that now applicable to a nuclear power plant, to include additional intruders, heavy weapons, aircraft attack, lethal chemical weapons and more than one vehicle bomb; and
- (v) any ISFSI on the site to receive protection equivalent to that provided for a nuclear power plant.

### *Facility Robustness*

Facility-robustness measures are those that improve the ability of a nuclear facility to experience destructive acts of malice or insanity without a significant release of radioactive material to the environment. In illustration, the PIUS reactor design, developed by the reactor vendor ASEA-Atom but never built, was intended to withstand aerial bombardment by 1,000-pound bombs without suffering core damage or releasing a significant amount of radioactive material to the environment.<sup>43</sup> A new reactor or ISFSI could be constructed with a similar degree of robustness.

At existing facilities, a variety of opportunities are available for enhancing robustness. As a high-priority example, the spent fuel pool(s) at a nuclear power plant could be re-equipped with low-density racks, so that spent fuel would not ignite if water were lost from a pool. As a second example, the reactor of a nuclear power plant could be permanently shut down, or the reactor could operate at reduced power, either permanently or at times of alert. Other robustness-enhancing opportunities could be identified. For a nuclear power plant whose reactor is not permanently shut down, robustness could be enhanced by an integrated set of measures such as:

- (i) automated shutdown of the reactor upon initiation of a high-alert status at the plant, with provision for completion of the automated shutdown sequence if the control room is disabled;
- (ii) permanent deployment of diesel-driven pumps and pre-engineered piping to be available to provide emergency water supply to the reactor, the steam generators (at a PWR) and the spent fuel pool(s);
- (iii) re-equipment of the spent fuel pool(s) with low-density racks, excess fuel being stored in an onsite ISFSI; and
- (iv) construction of the ISFSI to employ hardened, dispersed, dry storage.

### *Damage Control*

Damage-control measures are those that reduce the potential for a release of radioactive material from a facility following damage to that facility due to destructive acts of malice or insanity. Measures of this kind could be ad hoc or pre-engineered. One illustration of a damage-control measure would be a set of arrangements for patching and restoring water to a spent fuel pool that has been breached. Many other illustrations can be provided. It appears that the NRC has required licensees to undertake some planning for damage control following explosions or fires.<sup>44</sup> Additional measures would be appropriate. For example, at a site housing one or more nuclear power plants and an ISFSI, the following damage-control measures could be implemented:

---

<sup>43</sup> Hannerz, 1983.

<sup>44</sup> Meserve, 2002.

- (i) establishment of a damage-control capability at the site, using onsite personnel and equipment for first response and offsite resources for backup;
- (ii) periodic exercises of damage-control capability;
- (iii) establishment of a set of damage-control objectives -- to include patching and restoring water to a breached spent fuel pool, fire suppression in the ISFSI, and provision of cooling to a reactor whose support systems and control room are disabled -- with accompanying plans; and
- (iv) provision of equipment and training to allow damage control to proceed on a radioactively-contaminated site.

### *Offsite Emergency Response*

Emergency-response measures are those that reduce the potential for exposure of offsite populations to radiation, following a malice- or insanity-induced release of radioactive material from a nuclear facility. Measures in this category would in many respects be similar to emergency planning measures that are designed to accommodate "accidental" releases of radioactive material arising from human error, equipment failure or natural forces (e.g., earthquake). However, there are two major ways in which malice- or insanity-induced releases might differ from accidental releases. First, a malice- or insanity-induced release might be larger and begin earlier than an accidental release.<sup>45</sup> Second, a malice- or insanity-induced release might be accompanied by deliberate degradation of emergency response capabilities (e.g., the attacking group might block an evacuation route). Accommodating these differences could require additional measures of emergency response.

Overall, an appropriate way to improve emergency-response capability at a nuclear-power-plant site could be to implement a model emergency response plan that was developed by a team based at Clark University in Massachusetts.<sup>46</sup> This model plan was specifically designed to accommodate radioactive releases from spent-fuel-storage facilities, as well as from reactors. That provision, and other features of the plan, would provide a capability to accommodate both accidental releases and malice- or insanity-induced releases. Major features of the model plan include:<sup>47</sup>

- (i) structured objectives;
- (ii) improved flexibility and resilience, with a richer flow of information;
- (iii) precautionary initiation of response, with State authorities having an independent capability to identify conditions calling for a precautionary response<sup>48</sup>;

---

<sup>45</sup> Present plans for emergency response do not account for the potential for a large release of radioactive material from spent fuel, as would occur during a pool fire. The underlying assumption is that a release of this kind is very unlikely. That assumption cannot be sustained in the present threat environment.

<sup>46</sup> Golding et al, 1992.

<sup>47</sup> Ibid, pp 8-13.

<sup>48</sup> A security alert could be a condition calling for a precautionary response.

- (iv) criteria for long-term protective actions;
- (v) three planning zones, with the outer zone extending to any distance necessary<sup>49</sup>;
- (vi) improved structure for accident classification;
- (vii) increased State capabilities and power;
- (viii) enhanced role for local governments;
- (ix) improved capabilities for radiation monitoring, plume tracking and dose projection;
- (x) improved medical response;
- (xi) enhanced capability for information exchange;
- (xii) more emphasis on drills, exercises and training;
- (xiii) improved public education and involvement; and
- (xiv) requirement that emergency preparedness be regarded as a safety system equivalent to in-plant systems.

### *Protection of Spent-Fuel Shipments*

The preceding paragraphs of Section 6 outline a defense in depth for fixed nuclear facilities. A similar approach would be applicable to protecting spent-fuel shipments. For these shipments, the analog to site security would consist of measures to reduce the risk of attack, including: (i) selection of transport mode (road, rail or water) and route (proximity to population centers, etc.); (ii) a larger and more capable guard force; and (iii) deferral of transport until the global threat environment has moderated. The analog to facility robustness would be a spent-fuel container and/or overpack that is more robust against attack. Damage-control measures would include preparations for extinguishing a fire in spent-fuel cladding and reducing the release of radioactive material from a breached container; these actions might need to be automated. Emergency-response measures would include increased response capabilities in communities along the transport routes. Improved capabilities for responding to releases from fixed facilities, as outlined above, would allow more effective responses to releases during shipment of spent fuel.

## **7. Efforts by local and state governments and citizens to obtain protection**

Local and state governments and citizen groups have repeatedly sought improved protection against potential releases of radioactive material from nuclear reactors or spent fuel. Typically, this involves intervening in a license proceeding. Sometimes the effort has focussed on the potential for accidental releases of radioactive material, at other times on the potential for releases arising from acts of malice or insanity. A selected review of this experience is provided here, focussing on recent efforts to obtain improved protection against maliciously-induced releases.

---

<sup>49</sup> The inner and intermediate zones would have radii of 5 and 25 miles, respectively. As an example of the planning measures in each zone, potassium iodide would be predistributed within the 25-mile zone and made generally accessible nationwide.

*The Harris Plant*

The Harris plant in North Carolina features one nuclear reactor and four spent-fuel pools. Progress Energy, the licensee, uses these pools to store spent fuel discharged from the Harris reactor and spent fuel transported to the site from Progress Energy's Brunswick and Robinson reactors. Two pools have been in use since the Harris reactor began operating in 1987. The licensee applied to the NRC for a license amendment in late 1998, requesting permission to use the remaining two pools.

In response, Orange County, North Carolina, commissioned IRSS to prepare a report on the risk associated with the spent-fuel pools at Harris.<sup>50</sup> This report described the potential for a spent-fuel-pool fire, and identified acts of malice as potential causes of such a fire. In order to obtain for the public a better understanding of the risk of a pool fire and the options for reducing that risk, Orange County intervened in the license amendment proceeding, calling upon the NRC to prepare an environmental impact statement (EIS). During the proceeding, Orange County was not allowed to discuss acts of malice. Eventually, in March 2001, the NRC's licensing board denied the County's request for an evidentiary hearing to debate the need for an EIS. This decision was subsequently upheld by the NRC Commissioners and then by the US Court of Appeals. Thus, the two previously-unused pools at Harris entered service without an EIS being prepared. In fact, no EIS has ever considered the potential for a spent-fuel-pool fire.

Orange County's efforts were not, however, in vain. Two important outcomes have occurred, and the story is not yet finished. First, the County's intervention forced the NRC Staff to concede the role of flow blockage in the development of a spent-fuel-pool fire, thus correcting a major technical error in which the Staff had persisted for two decades.<sup>51</sup> Second, the citizen group NC-WARN has continued to educate the public about the risks associated with high-density pool storage and spent-fuel transportation, and the options for reducing those risks.<sup>52</sup> This effort has had some effect. In April 2003 Progress Energy announced that it is exploring the construction of dry-storage ISFSIs at its Robinson and Brunswick sites, implying that shipment of spent fuel to the Harris site will be phased out.

*EISs and Acts of Malice*

After the attacks of September 2001 on the World Trade Center and the Pentagon, many people saw a need for systematic assessments of: (i) the risks of maliciously-induced releases of radioactive material from nuclear facilities; and (ii) options for reducing those risks. Several citizen groups and the State of Utah intervened in five separate NRC license proceedings, calling for EISs to be prepared in order to meet this need. In two cases the intervenors explicitly recognized the importance of limiting the distribution of

---

<sup>50</sup> Thompson, 1999.

<sup>51</sup> Thompson, 2002, paragraph II-10.

<sup>52</sup> See, for example: Goff, 2003.

sensitive information about nuclear-facility vulnerabilities, and proposed an approach for addressing this problem in the context of a license proceeding and an EIS.

Utah's call for an EIS occurred in the context of the license proceeding for the proposed Skull Valley ISFSI. The Mothers for Peace made the same call in the context of a proposed ISFSI at the Diablo Canyon site.<sup>53</sup> Other citizen groups called for EISs in the context of license proceedings related to the Millstone 3, McGuire 1&2 and Catawba 1&2 nuclear power plants and a proposed mixed-oxide (MOX) fuel fabrication facility. In each of the five cases, the NRC dismissed the intervenor's call for an EIS, using the same rationale in each instance.<sup>54</sup> California Attorney General Bill Lockyer has stated that the NRC's rationale "is flawed, and will not survive judicial scrutiny".<sup>55</sup> The Mothers for Peace intends to seek such scrutiny from the US Court of Appeals.

These five cases were dismissed without any evidentiary hearing being held to debate the need for an EIS. Thus, the intervenors were unable to cross-examine expert witnesses from the NRC and the nuclear industry, and the intervenors' expert witnesses were denied an opportunity to present and defend their findings. The same was true in the Harris intervention described above.

#### *Letter from 27 Attorneys-General*

In October 2002, the Attorneys-General of 27 States sent a letter to the majority and minority leaders of the US Senate and House of Representatives.<sup>56</sup> The letter called for "passage of legislation this year to protect our states and communities from terrorist attacks against nuclear power plants and other sensitive nuclear facilities". Special attention was drawn to the vulnerability of spent-fuel pools. The Congress has not yet acted on this letter.

#### *Conclusion*

From this brief review, it is clear that local and state governments and citizen groups have sought improved protection for nuclear facilities against attack, but have been rebuffed by the NRC. Their interventions in license proceedings have been dismissed by the NRC

---

<sup>53</sup> In a separate effort, the Mothers for Peace has joined with the Union of Concerned Scientists in submitting to the NRC a petition for rulemaking, calling for better protection against radiological sabotage of nuclear power plants. See: MFP/UCS, 2003.

<sup>54</sup> Calls for EISs by Utah and three sets of citizen groups were dismissed by the NRC in December 2002, and the call by the Mothers for Peace was dismissed in January 2003.

<sup>55</sup> Letter from Bill Lockyer, Attorney General of California, to Richard Meserve, Chairman of the NRC, 28 February 2003, page 5.

<sup>56</sup> Letter from the Attorneys-General of Arizona, Arkansas, California, Colorado, Connecticut, Georgia, Hawaii, Iowa, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Montana, Nevada, New Jersey, New Mexico, New York, North Carolina, Ohio, Oregon, Pennsylvania, Rhode Island, Vermont, West Virginia, Washington and Wisconsin to the Senate Majority and Minority Leaders, the Speaker of the House and the House Minority Leader, 8 October 2002.

before even reaching the stage of an evidentiary hearing. They have also sought action through channels that bypass the NRC, with limited success to date.

## **8. Policy initiatives that are needed**

Three policy initiatives would be especially helpful in obtaining improved protection of nuclear facilities and operations. Each of these initiatives could be taken by the executive branch of the federal government, acting under current law. Alternatively, Congress could require the executive branch to take these actions. Ideally, both branches of government would cooperate to introduce these initiatives.

### *Replacing 10 CFR 50.13*

Since 1967, when the NRC's regulation 10 CFR 50.13 was promulgated, licensees are not required to design or operate nuclear facilities so as to resist attack by an enemy, "whether a foreign government or other person". Although this policy has been modified, nuclear sites remain lightly defended. In the present global threat environment, 10 CFR 50.13 is overdue for repeal and replacement by regulations that address nuclear-facility protection in the context of national security.

During the development of regulations to replace 10 CFR 50.13, we would need to debate the respective roles of licensees and government (federal, state and local) in protecting nuclear facilities and operations. There are limits to the type of protection that licensees can reasonably be asked to provide directly. For example, if automated missiles were deployed to destroy aircraft closing on a nuclear site, this deployment should be done by the federal government. One must then decide how to allocate the costs of protective measures that are not taken directly by a licensee. A possible resolution of this question would be for the federal government to bear such costs until present licenses expire or are transferred, while licensees would bear the full cost of protection after license transfer or during any period of license extension. This approach would recognize that current licenses were granted while 10 CFR 50.13 was in force, while ensuring that licensees pay the true costs of nuclear operations in the longer term.

### *Preparing EISs that Consider Acts of Malice or Insanity*

In five separate nuclear licensing cases, Utah and a variety of citizen groups have formally called upon the NRC to prepare EISs that assess : (i) the risks of maliciously-induced releases of radioactive material from nuclear facilities; and (ii) options for reducing those risks. The NRC has dismissed all five cases without even allowing an evidentiary hearing to debate the merits of the intervenors' requests. By taking this action, the NRC has denied the nation and the intervenors an opportunity to debate neglected issues that are central to national security. With or without a court ruling to this effect, the NRC should reverse its decision and prepare EISs. This application of EISs could be supplemented later by the use of security impact statements (see below).

### *Security Impact Statements*

In the present global threat environment, the risk of attack on our nuclear facilities and similar critical targets is predominantly from attacks that have a broad strategic purpose. The objective of an attack would probably be to create impacts on the homeland as a whole, the attacked facility itself perhaps being incidental to this purpose. Thus, reducing the risk of attack is a common-property task, analogous to protecting the environment.

These considerations have led two analysts to propose the introduction of security impact statements (SISs) that are analogous to EISs.<sup>57</sup> They propose that the SIS process should be the "operational heart" of the Department of Homeland Security, facilitating the making of strategic, cost-effective decisions about investments in the protection of critical targets. At present, there is no methodology to support such rational decision-making.

The SIS process could be valuable in the context of protecting nuclear facilities and other critical targets. It could be initiated by the Department of Homeland Security, and formalized by Congress through appropriate legislation. In the SIS process, the NRC would be a contributor of information, but the overall responsibility for preparing an SIS should rest with the Department of Homeland Security.

## **9. Establishing an independent technical capability**

The level of protection that we give to nuclear power plants and spent fuel is a national-security issue of great importance. Therefore, it is crucial that we obtain the best possible assessments of the potential for attack, the vulnerabilities of nuclear facilities and operations, and the options for providing improved protection. Findings from these assessments should guide our decisions about which protective measures we adopt, and should also inform the implementation of those measures.

### *Obtaining a Thorough, Unbiased Assessment*

Experience in assessing the safety of nuclear facilities (i.e., the potential for an accident not attributable to malice or insanity) has shown that obtaining the best possible assessment of safety is a difficult undertaking.<sup>58</sup> In the nuclear-safety arena the technical issues are complex. Scientific knowledge is often incomplete and empirical data are often unavailable, so that judgements must be made. In theory, the judgements are made by scientists in a purely objective way. In practice, large financial investments, careers, and institutional interests are affected by the findings of an assessment. These factors inevitably introduce bias, which is often unconscious. Also, analysts often experience

---

<sup>57</sup> Gale and Husick, 2003.

<sup>58</sup> See, for example: Ford, 1982; and Okrent, 1981.

pressure from decision-makers to portray the findings of an assessment as being more definitive and comprehensive than they truly are.

In the nuclear-security arena, the pressures toward bias in an assessment are even greater than in the nuclear-safety arena. Technical issues are more complex and empirical data are scarcer. The work is psychologically demanding. Engineers who may have devoted their professional lives to building nuclear facilities must imagine the deliberate misuse or destruction of those facilities. In assessing the potential for attack, analysts must contemplate a level of commitment on the part of attackers that is difficult to imagine. The findings of a nuclear-security assessment have at least as large an effect on investments, careers and institutional interests as do the findings of a nuclear-safety assessment.

### *Correcting Bias*

In the nuclear-safety arena, there have been two major antidotes to bias in assessments. One antidote is experience with actual accidents (e.g., Chernobyl) or near-accidents. This experience provides a reality check. The second antidote is public scrutiny of assessments, which can occur because the assessments have been published.

In the nuclear-security arena, both of these antidotes have been ineffective. To date, there has been no attack on a nuclear facility in the United States, a situation that one hopes will continue. Thus, experience has not yet provided a reality check. Public scrutiny of assessments is impossible because they have been conducted in secret by the nuclear industry and the NRC. Moreover, the NRC has refused to listen to the concerns of independent experts.<sup>59</sup> The resulting bias has been in the direction of under-estimating the potential for attack and the vulnerability of nuclear facilities to attack.<sup>60</sup>

### *An Independent Technical Capability*

To correct for bias, the nation needs an independent capability for review of threat assessments, vulnerability assessments and plans for protective measures. Experts who provide this review should be from institutions that are entirely independent of the nuclear industry and the NRC. Appropriate experts are available, as discussed below. Assistance could be obtained from the national laboratories, which are bountiful sources of expertise. However, the contractual arrangements for obtaining this expertise should be entirely separate from any arrangements the laboratories have with the NRC. Serving or retired special-forces soldiers could also be important sources of information.

An appropriate sponsoring body for this independent capability would be a consortium of state governments. Attorneys General might be the appropriate officials to represent

---

<sup>59</sup> MFP/UCS, 2003.

<sup>60</sup> In illustration of the NRC's bias toward under-estimation, see: NRC, 2003; MFP/UCS, 2003; and a letter of 17 March 2003 from former NRC staff member Joe Hopenfeld to Congressional staff.

states in this consortium. State governments are appropriate sponsors for at least three reasons. First, states already have responsibilities and capabilities in the nuclear-security arena. Second, state governments are more accessible to citizens than is the NRC, and are therefore more likely to gain respect and trust from the public. Third, the diversity of views that would be represented in a consortium of states would counteract tendencies toward bias.

Funding to support the independent technical capability should come from the federal government. Although funds might pass through a federal agency (e.g., Department of Energy, Department of Homeland Security, NRC), they should be provided in a manner that ensures true independence. This would require some Congressional action.

The necessary expertise could be found in universities and other independent organizations, with assistance from national laboratories and the military. Some examples illustrate the available expertise. Clark University has developed a model plan for offsite emergency response.<sup>61</sup> Experts from Princeton University, MIT and elsewhere have studied the risks of storing spent nuclear fuel.<sup>62</sup> Purdue University has a sophisticated capability for modelling the structural effects of aircraft impact.<sup>63</sup>

#### *Sensitive Information*

Assessments in the nuclear-security arena will generate and require information that is not always appropriate for unrestricted publication. However, it does not follow that assessments should be conducted in total secrecy, which has become the NRC's practice. Such secrecy breeds complacency and promotes bias, a tendency which the NRC compounds by refusing to listen to independent experts.

The proposed consortium should provide opportunities for concerned parties to submit information, with assurance that sensitive information will be treated appropriately. Also, the consortium should sponsor studies by experts who do not possess or seek security clearances. There are numerous experts who are capable of conducting studies that rely entirely on publicly-available information but will yield information that may be sensitive. At present, these experts lack opportunities to conduct such studies in a responsible manner, and must watch in frustration while nuclear-industry bodies proffer misleading information.

When the consortium issued findings, some information would necessarily be withheld from published documents. In such instances, the credibility of the findings would rest upon the perception of the consortium's independence, integrity and responsiveness to public concerns. A consortium of state governments has the potential to gain and hold the public's trust in these respects.

---

<sup>61</sup> Golding et al, 1992.

<sup>62</sup> Alvarez et al, 2003.

<sup>63</sup> Purdue, 2002; Sozen et al, 2002.

## **10. References**

(Alvarez et al, 2003)

Robert Alvarez and seven other authors, "Reducing the Hazards from Stored Spent Power-Reactor Fuel in the United States", Science and Global Security, 11:1-51, 2003.

(Baker, Cutler et al, 2001)

Howard Baker and Lloyd Cutler (co-chairs, Russia Task Force) et al, A Report Card on the Department of Energy's Nonproliferation Programs with Russia (Washington, DC: Secretary of Energy Advisory Board, US Department of Energy, 10 January 2001).

(Brian, 2003)

Danielle Brian, Executive Director, Project on Government Oversight, speech to the NRC's Regulatory Information Conference, 16 April 2003, available at <<http://www.pogo.org/p/environment/et-030401-nuclear.html>>, accessed 24 May 2003.

(Chapin et al, 2002)

Douglas M. Chapin et al, "Nuclear Power Plants and Their Fuel as Terrorist Targets", Science, Volume 297, 20 September 2002, pp 1997-1999.

(Collins et al, 2000)

Timothy Collins et al, Technical Study of Spent Fuel Pool Accident Risk at Decommissioning Nuclear Power Plants (Washington, DC: US Nuclear Regulatory Commission, October 2000).

(DOE, 2002)

US Department of Energy, Final Environmental Impact Statement for a Geologic Repository for the Disposal of Spent Nuclear Fuel and High-Level Radioactive Waste at Yucca Mountain, Nye County, Nevada, DOE/EIS-0250F (Washington, DC: DOE, February 2002).

(Ewing and Macfarlane, 2002)

Rodney C. Ewing and Allison Macfarlane, "Yucca Mountain", Science, Volume 296, 26 April 2002, pp 659-660.

(Ford, 1982)

Daniel Ford, Cult of the Atom (New York, New York: Simon and Schuster, 1982).

(Gale and Husick, 2003)

Stephen Gale and Lawrence Husick, "From MAD (Mutual Assured Destruction) to MUD (Mutual Unconstrained Disruption): Dealing with the New Terrorism", Foreign Policy Research Institute Wire, Volume 11, Number 1, February 2003.

(Goff, 2003)

Stanley A Goff, Predeployed Radiological Weapon: Reducing the targetability of Shearon Harris Nuclear Plant and the risk to the North Carolina public (Durham, North Carolina: NC-WARN, 1 May 2003).

(Golding et al, 1992)

Dominic Golding et al, Managing Nuclear Accidents: A Model Emergency Response Plan for Power Plants and Communities (Boulder, Colorado: Westview Press, 1992).

(Hannerz, 1983)

K. Hannerz, Towards Intrinsically Safe Light Water Reactors (Oak Ridge, Tennessee: Institute for Energy Analysis, February 1983).

(Hart et al, 2002)

Gary Hart and Warren B. Rudman (co-chairs), Stephen E. Flynn (project director) and Task Force members, America Still Unprepared -- America Still in Danger: Report of an Independent Task Force Sponsored by the Council on Foreign Relations (New York, NY: Council on Foreign Relations, 25 October 2002).

(Hirsch et al, 2003)

Daniel Hirsch, David Lochbaum and Edwin Lyman, "The NRC's Dirty Little Secret", Bulletin of the Atomic Scientists, May/June 2003, pp 45-51.

(Jones, 2002a)

David Jones, "Sandia says its study not proof of nuke plant durability" Inside Energy, 30 September 2002, page 14.

(Jones, 2002b)

Gary Jones, Director, Natural Resources and Environment, US General Accounting Office, "Nuclear Waste: Uncertainties about the Yucca Mountain Repository Project", testimony before the Subcommittee on Energy and Air Quality, House Committee on Energy and Commerce, 21 March 2002.

(Macfarlane, 2001a)

Allison Macfarlane, "Interim Storage of Spent Fuel in the United States", Annual Review of Energy & Environment, Volume 26 (2001), pp 201-235.

(Macfarlane, 2001b)

Allison Macfarlane, "The problem of used nuclear fuel: lessons for interim solutions from a comparative cost analysis", Energy Policy, Volume 29 (2001), pp 1379-1389.

(Markey, 2002)

Staff of US Representative Edward Markey, "Security Gap: A Hard Look At the Soft Spots in Our Civilian Nuclear Reactor Security", 25 March 2002.

(Meserve, 2003)

NRC Chairman Richard Meserve, letter to Tom Ridge, Secretary of Homeland Security, 31 March 2003. Note: This letter, when downloaded from the NRC website ([www.nrc.gov](http://www.nrc.gov), accessed by IRSS on 23 May 2003), is packaged with a letter of 5 September 2002 from Meserve to Ridge.

(Meserve, 2002)

NRC Chairman Richard Meserve, "Statement Submitted by the United States Nuclear Regulatory Commission to the Committee on Environment and Public Works, United States Senate, Concerning Nuclear Power Plant Security", 5 June 2002.

(MFP/UCS, 2003)

Mothers for Peace and Union of Concerned Scientists, Petition [to the NRC] for Rulemaking, 28 April 2003.

(NAC, 2001)

NAC Worldwide Consulting, US Spent Fuel Update: Year 2000 in Review (Atlanta, Georgia: NAC Worldwide Consulting, 2001).

(NRC, 2003)

US Nuclear Regulatory Commission, "Briefing on the Status of Office of Research (RES) Programs, Performance, and Plans", transcript of an open session of the Commission, Rockville, Maryland, 27 March 2003.

(NRC, 2002)

US Nuclear Regulatory Commission, Fact Sheet: Nuclear Security Enhancements Since Sept. 11, 2001 (Washington, DC: US Nuclear Regulatory Commission, undated, apparently September 2002).

(NRC, 1990)

US Nuclear Regulatory Commission, Severe Accident Risks: An Assessment for Five US Nuclear Power Plants, NUREG-1150 (Washington, DC: US Nuclear Regulatory Commission, December 1990).

(Office of Homeland Security, 2002)  
Office of Homeland Security, National Strategy for Homeland Security (Washington, DC: The White House, July 2002).

(Okrent, 1981)  
David Okrent, Nuclear Reactor Safety (Madison, Wisconsin: University of Wisconsin Press, 1981).

(Pew, 2003)  
Pew Research Center for the People and the Press, Views of a Changing World 2003 (Washington, DC: Pew Research Center, 3 June 2003).

(POGO, 2002)  
Project on Government Oversight, Nuclear Power Plant Security: Voices from Inside the Fences (Washington, DC: Project on Government Oversight, 12 September 2002).

(Purdue, 2002)  
Purdue University, "Purdue News: New simulation shows 9/11 plane crash with scientific detail", 10 September 2002.

(Scarry, 2002)  
Elaine Scarry, "A nuclear double standard", Boston Sunday Globe, 3 November 2002, page D11.

(Sozen et al, 2002)  
Mete A. Sozen et al, "September 11 Pentagon Attack Simulations Using LS-Dyna: Phase I, Completed September 11, 2002", available at  
<<http://www.cs.purdue.edu/homes/cmh/simulation/>>.

(Sprung et al, 2000)  
J. L. Sprung et al, Reexamination of Spent Fuel Shipment Risk Estimates, NUREG/CR-6672 (Washington, DC: US Nuclear Regulatory Commission, March 2000).

(Thompson, 2003)  
Gordon Thompson, Robust Storage of Spent Nuclear Fuel: A Neglected Issue of Homeland Security (Cambridge, Massachusetts: Institute for Resource and Security Studies, January 2003).

(Thompson, 2002)  
Gordon Thompson, Declaration of 7 September 2002 in support of a petition to the US Nuclear Regulatory Commission by Avila Valley Advisory Council et al, regarding nuclear-facility operations at the Diablo Canyon site.

(Thompson, 1999)

Gordon Thompson, Risks and Alternative Options Associated with Spent Fuel Storage at the Shearon Harris Nuclear Power Plant (Cambridge, Massachusetts: Institute for Resource and Security Studies, February 1999).

(White House, 2003)

The White House, The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets (Washington, DC: The White House. February 2003).

(White House, 2002)

The White House, The National Security Strategy of the United States of America (Washington, DC: The White House, September 2002).

\*\*\*\*\*