



# Security at Nuclear Power Plants in the Post-September 11<sup>th</sup> Environment

by  
Jennifer Miller  
The Ohio State University

Prepared for the  
Washington Internships for Students of Engineering  
Sponsored by the  
American Nuclear Society

August 2002



## **Table of Contents**

---

About the Author.....	3
About WISE.....	3
Acknowledgements.....	3
Executive Summary.....	5
Introduction.....	7
Security Basics.....	8
Effects of September 11, 2001.....	13
Keys to an Effective Security Program.....	16
Current Debate.....	21
Regulatory.....	21
Legislative.....	24
Recommendations to Relevant Agencies and Organizations.....	30
Conclusions.....	37
Appendix A: List of Acronyms.....	39
Citations.....	40

## **About the Author**

---

Jen Miller is a senior at the Ohio State University in Columbus, Ohio. She is currently studying mechanical engineering with a specialization in nuclear engineering and a minor in business. Jen is a participant of the 2002 summer Washington Internships for Students of Engineering (WISE) program, under the sponsorship of the American Nuclear Society. This report culminates her extensive research effort on current policy issues related to physical security of commercial nuclear power plants.

## **About WISE**

---

The Washington Internships for Students of Engineering (WISE) program is a unique opportunity for engineering students to explore how science and technology affect public policy decisions. The 10-week Washington, DC, experience includes regular group meetings with a variety of government agencies and private organizations in the area. In addition to group functions, each student researches a technical issue of interest to the student and his professional society. The culmination of this research is the formulation of a final written report and presentation. To learn more about WISE, visit the program's website at <http://www.wise-intern.org/>.

## **Acknowledgements**

---

Many people have contributed their time and effort to assist my research and writing of this report. First and foremost is the American Nuclear Society, who has sponsored my internship here. Thank you to my advisor Dr. Alan Levin from the Nuclear Regulatory Commission for helping me formulate my topic and revising many drafts. I also thank our Dr. Jim Dennison, our WISE faculty member in residence. In addition to group leadership, Dr. Dennison spent many hours helping me prepare for my final presentation.

The Nuclear Energy Institute has been extremely generous in providing office space and supplies, in addition to technical resources crucial to my research. Special thanks to Sherry Reilly and Sonja Simmons for their support at NEI. Others who have provided technical assistance are Doug Walters, Lynnette Hendricks, and Jerry Slomenski.

I would also like to acknowledge my two officemates, Simon Lobdell and Wayne Blaylock, who have been great friends, advisors, and WISE-guys throughout the summer.

Finally, thank you to Mr. Brian Hajek and the nuclear engineering faculty at the Ohio State University for fostering my interest in nuclear studies and helping me in my career development.

## Executive Summary

---

The events of September 11<sup>th</sup>, 2001, call for a re-examination of all aspects of homeland security. Nuclear power plants are generally included in a group of critical infrastructures including dams, bridges, water supplies, chemical and biological facilities, electrical grids, and so forth, which must be secured. The nuclear industry has long maintained that it is a model for effective security in private infrastructure sectors. The general public, however, remains largely uninformed and therefore skeptical about the safety and security of nuclear facilities. This report is intended to address the public's heightened concerns since September 11<sup>th</sup>.

The Nuclear Regulatory Commission (NRC) oversees each reactor licensee's<sup>1</sup> ability to adequately protect against a minimum threat level, called the design basis threat. To do this, licensees employ a number of protection methods. These include concentric rings of increasingly stringent security layers around the plant, numerous layers of structural design around the reactor core, a heavily regulated private security force, and rigorous testing methods for security and emergency response plans.

Since September 11<sup>th</sup>, much has been done to elevate the level of security at the plants. The NRC has issued advisories and interim compensatory measures for licensees to bring their security to the highest level of alert, where it remains today. The Commission has created a new Nuclear Security and Incident Response office and instigated a "top-to-bottom" review of all security related policies and procedures. Federal, state, and local governments have also offered assistance of some form.

An effective commercial security program, whether in the nuclear industry or any other aspect of critical infrastructure, utilizes certain essential tools. These include written procedures, communication and interagency collaboration, testing and evaluation methods, and continuous re-evaluation of the threat environment. The nuclear industry employs all of these methods; however, in accord with the national homeland security initiative, every effort should be made to strengthen the system and identify areas for improvement.

---

<sup>1</sup> owner of a commercial nuclear facility

There is a need for all parties associated with nuclear security to understand the division of responsibilities between licensees and federal, state, and local government. The current issues under regulatory and legislative debate right now essentially reflect the effort to clarify these lines of responsibility. Some general considerations can be made about how the various government agencies and the nuclear industry can facilitate this process.

The NRC should act as quickly as possible to complete its top-to-bottom security review and also expand it into an ongoing effort after post-September 11<sup>th</sup> issues have been addressed. It is hoped that President George W. Bush's proposed Department of Homeland Security will take the lead in organizing better collaboration between federal agencies and the licensees. No such system is in place on a state level, so it is the responsibility of the licensees and also state and local governments to take the initiative locally. Congress, too, has an important role. In the midst of tremendous legislative activity regarding homeland security, Congress must be especially careful to distinguish between the needs of the nuclear industry and those of other aspects of critical infrastructure.

## Introduction

---

Throughout the nearly 50-year history of nuclear power, public interest in matters of safety and security at nuclear sites has been intense. Among the concerns of the public has been the possibility of a large radiological release to the surrounding environment. While the majority of public concern was initially for accidental incidents, deliberate acts of sabotage also constituted an increasingly plausible fear. Events such as the 1993 World Trade Center bombing and the 1995 Oklahoma City bombing made people more aware of the vulnerability of public sites to acts of sabotage. Nuclear facilities, already in the public eye, were certainly one category of perceived targets. The ultimate act of sabotage, the terrorist attacks on September 11, 2001, redefined the realm of possibilities. The national priority has become re-examining all aspects of the nation's defense capabilities, both public and private.

Following September 11<sup>th</sup>, the possibility of airborne attack on a nuclear facility received significant attention from both the public and government officials. Attention has been on whether plants are prepared to defend against such events, and if not, what policies need to be implemented to improve defense capabilities. This has sparked an even wider discussion on a whole range of issues related to nuclear facility security. These issues call for a re-evaluation of the entire security framework, which includes not only the plant owners, but also regulators, federal agencies, state and local governments, emergency response organizations, and other important parties. These groups are involved in security-related activities such as physical design, security personnel, policy-making, regulating, and emergency response planning.

This report will highlight the current security framework, the changes needed for improving security, and the methods in which to implement these changes. The most important task is organizing all of the responsible parties so that they can work together most effectively. Thus, a major theme of this report is the integration of resources and each party's responsibility in the overall organizational effort.

## Security Basics

---

This section explains the basic security framework, as it existed before September 11<sup>th</sup>. The overall security picture includes, but is not limited to, the topics discussed here. The purpose of this section is to gain understanding of the current system, in order to evaluate what changes need to be made for the future.

### *The Design Basis Threat*

Since its inception as a purely regulatory body in 1974, the United States Nuclear Regulatory Commission (NRC) has had oversight responsibilities for each reactor licensee to adequately protect against the design basis threat (DBT). Defined in the Code of Federal Regulations (10 CFR 73.1), the DBT is a description of scenarios including the number of attackers, modes of attack, and weapons of attack against which a nuclear facility must be able to defend.<sup>2</sup> It is generally described as the reasonable level of protection for which the plant owner is legally responsible. Beyond the DBT, the NRC has determined that either the probability of an occurrence is too low or the responsibility of protection belongs to another party (the government). Power plant sites utilize a number of diverse, redundant security systems in order to protect against the design basis threat. In fact, licensees almost always go beyond the minimum standards of protection called for by the DBT.

### *Site Security Layers*

“Defense in depth” is the common phrase used in the nuclear energy industry to describe the exhaustive system of physical security in place at each of the United States’ 104 commercial nuclear reactors. Site protection begins with a number of concentric rings of security, shown in Figure 1. The first layer of security is the “owner-controlled area,” which generally includes patrolling and restricted vehicle access. This line encloses all property associated with the plant, and is typically a few miles in radius away from the plant. Inside the owner-controlled area is a stricter layer of security, the “protected area.” Standard protection devices here include a double

---

<sup>2</sup> The specific details of the DBT are classified for information security purposes.

fence, barbed wire, microwave detection equipment, and high tech cameras. Only one access control point is available along the protected area border, and an entering person must either be accompanied by appropriate security personnel or obtain a computer-coded badge issued by the security force. Also, all vehicles are subject to search before entering. The innermost layer of security at a nuclear plant is called the “vital area.” This includes all of the necessary equipment for safe operation and shutdown of the reactor. Access requirements at this layer of security are even more stringent and detection equipment is more sophisticated.

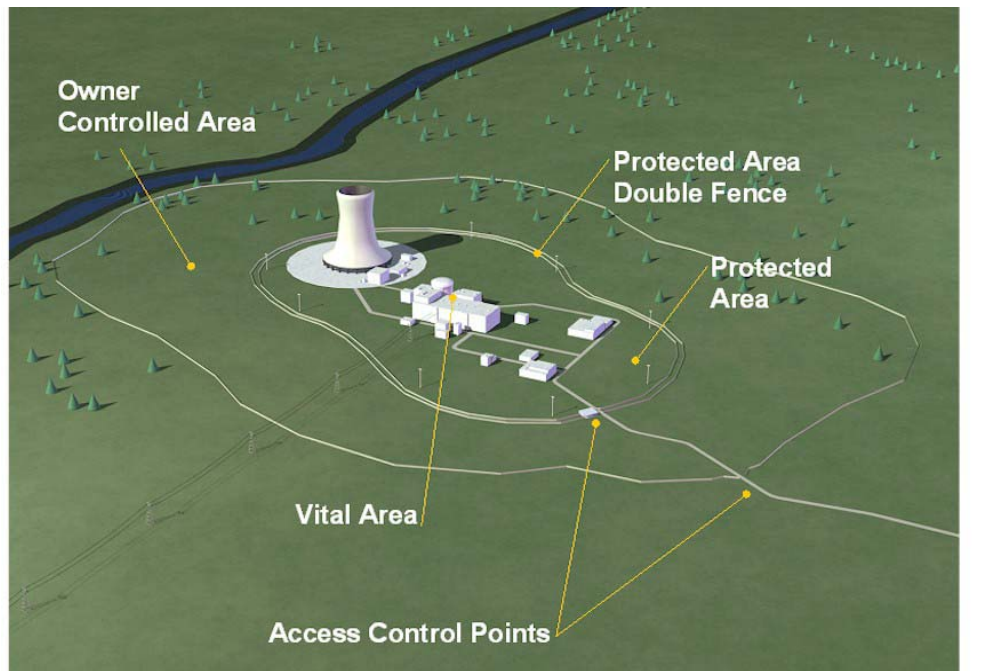


Figure 1: Nuclear Plant Security Area<sup>3</sup>

### *Physical Design of Plants*

Within the vital area, the plant itself provides for a high degree of security protection by design. This includes detailed plant shutdown systems and redundant backup systems for all vital safety equipment in case of emergency. Redundant structures, systems, and components are physically located at opposite areas of the plant.

---

<sup>3</sup> [http://www.nei.org/documents/Nuclear\\_Plant\\_Security\\_Zones.ppt](http://www.nei.org/documents/Nuclear_Plant_Security_Zones.ppt)

Protection against the release of radioactive material, which would come from the reactor core, is provided by numerous layers of structural design, shown in Figure 2 for a typical boiling water reactor design.<sup>4</sup> The first layer is the fuel itself, which is a ceramic material designed to hold in radioactive byproducts. Next are the fuel rods, or cladding, which fully encompass the nuclear fuel in stainless steel tubing. Containing all of the fuel assemblies is the reactor vessel, a larger steel structure 4-8 inches thick. Outside of the vessel are other protective structures, such as a 5-foot thick reinforced concrete dry well wall and 4-foot thick biological shield. The final outer layer is the containment wall, which has a 1.5-inch thick steel lining inside a 3-foot thick reinforced concrete shield wall. All of these protective barriers make physical penetration of the reactor or radiological release due to accidents in the core a highly improbable event.

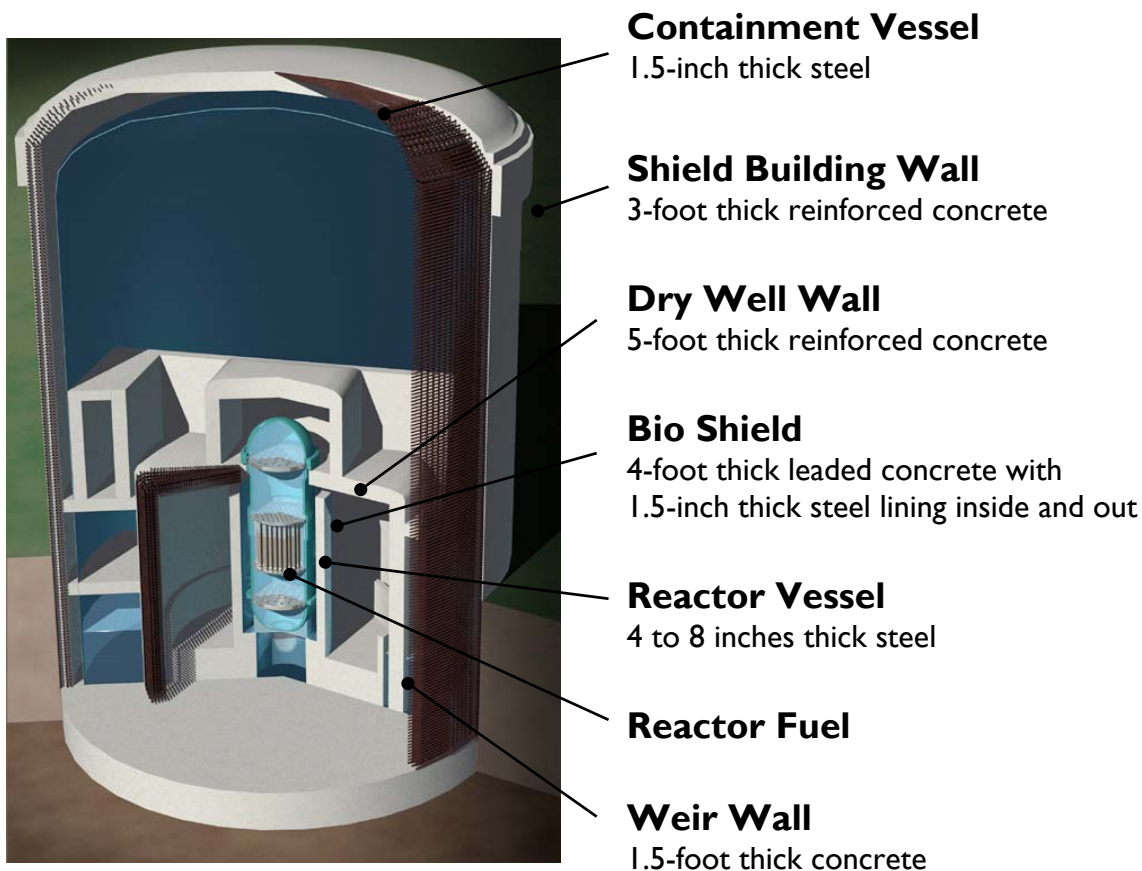


Figure 2: Physical Design<sup>5</sup>

<sup>4</sup> There are 35 boiling water reactors in the US; the other 69 reactors are pressurized water reactors, which have different design characteristics but the same level of barrier protection.

<sup>5</sup> <http://www.nei.org/documents/multilayershires.htm>

## *Security Forces*

Aside from physical barriers, the most critical aspect of nuclear power plant security is the security staff itself. As required by the NRC under 10 CFR 73, a plant owner must either provide or contract for a robust security force that meets specific standards and is capable of protecting against specific threat scenarios. Security personnel are subject to FBI background checks, physical and psychological testing, and continuous fitness-for-duty testing, among other requirements. Many of them have prior law enforcement or military experience, and all of them go through training and annual reexaminations in over 70 security-related topics.<sup>6</sup> 10 CFR 73.55 also requires that the licensee develop a formal security response plan, subject to the NRC's approval, and incorporate relevant state and local agencies in its coordination plans. Periodically, the security force is tested on its readiness for deployment of these plans, which is explained in the following paragraph.

### *Force-on-Force Testing*

The NRC employs resident inspectors at every plant at all times to ensure that the licensee is complying with regulatory standards. In addition to this oversight, the NRC established in 1991 the Operational Safety and Response Evaluation (OSRE) to test and evaluate a plant's security response capability. This is a requirement of 10 CFR 73.55. During an OSRE exercise, NRC officials are on hand to observe and evaluate the security personnel's response to a full-scale mock attack by an independently hired adversary force. This force is fully trained and receives detailed insider knowledge of plant layout and design before an exercise. After an OSRE exercise, the NRC can require the plant to make certain adjustments or improvements to its security plans as necessary.

In 1999, the NRC proposed a pilot program called Safeguards Performance Assessment (SPA) to shift away from OSRE and give greater responsibility to the industry. Licensees would be responsible for developing their test scenarios and conducting ongoing tests on a more frequent basis than was possible with the OSRE program. The individual tests would culminate in a

---

<sup>6</sup> "Implications of Security Force Federalization on Nuclear Power Plant Security." p. 9.

comprehensive NRC evaluation every three years, rather than every eight years with the OSRE system. In 2001, the Commission approved of a one-year, 8-plant pilot experiment of the SPA program to determine whether it should replace OSRE in the future; however, implementation of the SPA program is being re-evaluated as a result of September 11<sup>th</sup>. The pilot study has not commenced and the future of SPA is unclear.

### *Emergency Response*

After the accident at the Pennsylvania Three Mile Island plant in 1979, significant emphasis was placed on emergency response procedures surrounding the plant. Congress mandated that every plant develop and periodically test a comprehensive emergency response plan that covers a 10-mile Emergency Planning Zone (EPZ) around the plant. Under the NRC Authorization Act in 1980, the plans are subject to both the NRC and the Federal Emergency Management Agency (FEMA) approval for the plant to obtain and maintain its operating license.

Emergency response plans must also include the involvement of state and local assistance. Biannually, plants are required to conduct a full-scale test along with the relevant state and local agencies, under the watch of the NRC and FEMA. In addition, plants conduct their own training drills during off years. Outside of the 10-mile EPZ, FEMA has the lead role in emergency response efforts.<sup>7</sup>

---

<sup>7</sup> For more information, see “Emergency Preparedness Near Nuclear Power Plants.” Nuclear Energy Institute.

## The Effects of September 11, 2001

---

Similar to all other elements of critical infrastructure in the United States, the nuclear industry responded quickly with provisional security enhancements after the terrorist attacks on September 11<sup>th</sup>, 2001. Both the government and industry took immediate action to be prepared to respond to another terrorist attack.

Within hours of the attacks, the NRC activated its Emergency Operating Center at the NRC headquarters and 4 regional Incident Response Centers. It issued a threat advisory to all licensees advising them to go to the highest level of security. Licensees promptly complied with the following measures:

- increased patrols, security posts, barriers, and other physical protections
- more stringent personnel access requirements
- vehicle checks moved further away from the plant
- increased communication with federal, state and local law enforcement and military resources

In the first 3 months following the attacks, the NRC issued approximately 30 advisories to the plants that addressed security enhancements such as these. Some advisories were industry-wide and others were tailored to individual plants or groups of plants. Some requests were more challenging than others, but across the board licensees were quick to comply with each request. In addition to complying with NRC advisories, licensees also took initiative to review and enhance their security plans.

On February 25, 2002, the NRC issued the first *mandatory* orders to the licensees, a set of interim compensatory measures (ICMs), to remain in effect until the Commission either determines that the threat level is sufficiently diminished, or that some long-term security changes are to be implemented. Some of the ICMs were simply formal definitions of the measures that plants had already implemented. Others were far more complex and involved long-term engineering analyses.<sup>8</sup> The NRC placed a deadline of August 31, 2002, for plants to complete their upgrades and currently all plants have indicated that they will meet the deadline.

---

<sup>8</sup> The details of the interim compensatory measures are classified for information security purposes.

The NRC also initiated a comprehensive “top-to-bottom” review of its security programs. One of the most significant results of this review to date has been the creation of the Office of Nuclear Security and Incident Response (NSIR). This move essentially combines all of the security, safeguards, and incident response functions of the Commission, which were previously scattered among the various NRC offices, into a single organization with common tasks and goals. Another important task in the Commission’s review has been extensive re-evaluation of the DBT to include greater threat possibilities. No official changes have been made to date, however a decision on redefining the DBT is expected by the fall of 2002.

State and local governments have also responded actively to concerns about nuclear security since September 11<sup>th</sup>. Some states initially called in National Guard troops to protect their plants after the attacks. Since the NRC advisories and ICMs have demanded more of the security personnel, many facilities deployed local law enforcement troops for regular on-site assistance. On the executive level, states have established new homeland security offices and task forces, which are working on comprehensive anti-terrorist legislation. Obviously these organizations are addressing all types of security fronts, but nuclear power plant safety is an important consideration in the 35 states that are home to plants.

The formulation of the executive Office of Homeland Security (OHS) on October 8<sup>th</sup>, 2001, has been another effect of September 11<sup>th</sup> that will affect nuclear security operations. According to OHS’s Bob Stephan, the primary role of the Office of Homeland Security from the outset has been coordination of multiple federal resources and legislative support for funding to facilitate urgent homeland security needs.<sup>9</sup> On June 6, 2002, President Bush proposed the Department of Homeland Security (DHS) as the largest addition to the federal government in over 50 years. In his proposed Homeland Security Act of 2002, Bush calls for reorganization of key federal agencies such as FEMA and the Coast Guard, both of which play important roles in nuclear security.

---

<sup>9</sup> Stephan, Bob. Personal interview. 4 June 2002.

Other concerns from members of Congress have been brought up as well. Understandably, the public and Congress are concerned that new types of terrorist threats pose previously unforeseen risks to plants operating under pre-September 11<sup>th</sup> security conditions. There has been significant legislative activity on issues of security force capability and readiness, as well the division of responsibilities. At this time, these bills and amendments are in committee and being evaluated by numerous federal agencies such as the NRC, Department of Energy, Department of Defense, FEMA, and representatives of the nuclear industry. The status and future of these bills will be discussed in more detail later in this report.

## Keys to an Effective Security Program

---

After the initial shock of September 11<sup>th</sup>, the public attitude has gradually shifted towards a more controlled, thorough analysis of our long-term security needs. The re-evaluation of many infrastructure industries leads into an examination of the key characteristics of an effective commercial security system. For each characteristic, the nuclear industry's involvement is highlighted. First, some important definitions are necessary.

### *Definitions*

A recent Brookings Institution report on homeland security delineates the differences between the functions prevention, protection, and mitigation in any type of security effort.<sup>10</sup> Prevention includes preemptive efforts such as intelligence gathering, weapons monitoring, threat assessment, and so forth. Protection is the physical actions necessary to withstand or deter an act of sabotage. Mitigation includes post-accident actions such as evacuation, medical or fire attention, and clean up. According to the report, general prevention is usually the responsibility of federal, state, and local government. Protection of a specific commercial site is the responsibility of the individual owner. Emergency response should be a collaborative effort, but state and local governments are the most capable organization for this responsibility.

The overall responsibility of the NRC is the “to protect public health and safety, the environment and the common defense and security.”<sup>11</sup> While protection of the plant's functional capability is not specifically regulated, it is understood that the licensee would take additional actions to protect its investment as well as that of the public.

It is important to note that when talking about nuclear plant security force responsibilities, “prevention” is only associated with measures taken to prevent damage to the plant, particularly that which would threaten a radiological release. Prevention does not incorporate measures to

---

<sup>10</sup> Protecting the American Homeland: A Preliminary Analysis. Brookings Institution Press. p. 9-11

<sup>11</sup> NUREG/BR-0099, Revision 10. The NRC's responsibilities were outlined in the Energy Reorganization Act of 1974.

prevent the possibility of an attack. This is out of the scope of a private security force, and should be treated as a separate issue.

### *Characteristics*

With the definitions of protection, prevention, and mitigation in mind, the next logical step is to describe the general characteristics of an effective nuclear security program. These characteristics are primarily based on common sense and established business practices. In fact, nuclear security forces have implemented these tactics successfully for years. In light of the new threat environment however, current tactics need to be scrutinized, refined, and perfected more than ever before.

#### 1.) *Written procedures*

In the event of a serious threat, timely and well-organized action is essential to ensuring proper response. Each individual must know or have access to his particular responsibility in every situation, and a pre-planned, well-documented set of procedures ensures that this will happen. On a broader level, written procedures are important for ensuring ownership of responsibility for each level of government and other parties that should get involved in security plans. In the past, two common problems that have resulted from unclear responsibilities include lack of a cohesive effort from within the federal government and the development of federal programs that were similar or duplicative to state and local programs.<sup>12</sup> With well-organized, integrated written commitments this type of confusion can be avoided.

Written procedures for nuclear facility security fall under the category of quality assurance criteria, discussed in 10 CFR 50, Appendix B. A plant must document the organization of its security force and each individual's roles and responsibilities. Various portions of NRC code call for written procedures on specific aspects of a plant's security plan, all of which are

---

<sup>12</sup> Yim, Randall A. "National Preparedness: Integration of Federal, State, Local, and Private Sector Efforts Is Critical to an Effective National Strategy for Homeland Security." p. 9-10.

subject to NRC's approval. These procedures cover a variety of security issues such as physical protection systems, personnel organization, threat assessment, incident response, and emergency planning.<sup>13</sup> The NRC establishes baseline requirements for security programs and each plant develops a unique plan tailored to its needs. On the federal level, however, the written procedures for a government agency's role in a nuclear security incident are not as clear.

## 2.) *Avenues of communication between necessary parties*

It is critical to a security response plan that when a threat arises every involved person has appropriate access to essential information; thus, a single point of contact for plants and a specific interagency command and control structure is necessary. Establishing clear command and control will help prevent a lack of communication between various parties that may cause confusion or slower response times. Plant employees need to know exactly who to take information from, when to take action on certain information, and who to call in case of certain emergencies. Inter-agency communication and collaboration is particularly important to an effective comprehensive response.

While no single agency is solely responsible for communicating threat information to nuclear plants, the framework for threat monitoring and information gathering is in place. On a day-to-day basis, nearly 70 federal agencies play a part in general homeland security.<sup>14</sup> The NRC

also has a threat assessment department, but communication with plants is difficult because very few plant employees have security clearance. Because so many agencies participate in security operations, critical information sharing is often a confusing procedure.<sup>15</sup>

## 3.) *Testing and evaluation methods*

---

<sup>13</sup> Generally found in 10 CFR 73.46

<sup>14</sup> Office of Management and Budget. *Annual Report to Congress on Combating Terrorism*. p. 89-100.

<sup>15</sup> Hendricks, Lynnette. Personal Interview. 6 June 2002.

A rigorous testing and evaluation system is necessary for providing an appropriate level of accountability. It is an important tool for ensuring the efficiency and effectiveness of a nuclear security program that, in all likelihood, will probably never be tested in a real situation. Most plants have never encountered a serious threat, so response to an actual security threat is hypothetical. As a general rule, quantifiable testing methods “allow the government to measure the preparedness of different parts of the country in a consistent and comparable way, providing a reasonable baseline against which to measure progress.”<sup>16</sup>

Testing and evaluation of nuclear plant security generally falls to the NRC. As discussed in the background information, a large part of this component consists of the NRC-directed Operational Safety and Response Evaluation (OSRE) program. Regardless of whether the move is made to the SPA system, it is clear that testing and evaluation has always been strongly emphasized from the regulatory perspective and will continue to be in the future. Plants also participate in more frequent testing on their own accord. This includes a variety of activities, from large-scale emergency response exercises to employee training and re-certification programs.

#### 4.) *Adaptability to the threat environment.*

The type of threats, the possibility of certain threats, and the risk associated with these threats are important in determining the level of security needed. Unfortunately, these factors are not constant at all times. As September 11<sup>th</sup> illustrated, the security of an entire country can change overnight. The threat environment needs to be continuously monitored, and security readiness needs to be periodically re-evaluated. This should happen at the federal level through intelligence gathering and threat monitoring agencies. Local threat environments may be different than the national level, however. Certain industries may at various times be more vulnerable than others. For this reason, all levels of government and industry need to be vigilant of their particular situation.

---

<sup>16</sup> Yim, Randall A. “National Preparedness: Integration of Federal, State, Local, and Private Sector Efforts Is Critical to an Effective National Strategy for Homeland Security.” p. 16

In the past, the NRC has changed the DBT as a result of current events outside the industry and re-evaluation of the threat environment. For instance a year after the World Trade Center bombing in 1993, the DBT was enhanced to protect against a truck bomb by increasing vehicle barriers and set back distances for vehicle check points. Although it has not been altered frequently, the NRC does continuously monitor the DBT in relation to the threat environment. Aside from defining the DBT, however, the NRC as a large regulatory body is not ideally suited for the detailed analyses that continuous re-evaluation requires. The DBT is the regulatory minimum. Being prepared for such a level does not automatically guarantee that the plant is safe from threat. It is important that some on-site system be in place to consistently and frequently assess a plant's readiness. This should be based on the ever-changing threat environment as well as the details of plant's security system. To centralize resources, this should also be the organization that makes the final decision as to how to respond to a threat. This is a responsibility currently left to the plants

Again, it is important to note that these four tools were already in place and well established at nuclear power plants prior to September 11, 2001; nevertheless, there is obvious justification at this time for the nation to re-examine the stability of its entire critical infrastructure scheme. The nuclear industry is just one of the many subjects of the government's current initiative on enhancing homeland security. Whether or not significant needs are determined to be necessary for nuclear power plants, the nation can only be strengthened by a thorough analysis of its security readiness on all fronts.

## **Current Debate**

---

Since September 11<sup>th</sup>, there has been much discussion on ways to improve or enhance security at nuclear power facilities. The wide range of suggestions represents understandable post-September 11<sup>th</sup> fears. Among the most demanding suggestions is one for complete shut down of all plants until licensees implement certain measures to guarantee deterrence of an airborne attack or other event of similar magnitude. Organizations such as the Nuclear Control Institute have called for anti-aircraft artillery and 30-40 National Guard troops to be permanently stationed at every facility.<sup>17</sup> While these arguments represent fair opinions, they have not garnered significant support from the scientific and policy-making communities. It should be noted that the arguments above deserve fair attention as they represent reasonable, justifiable concerns for public safety; however, following section will focus on the main issues that policy-makers are seriously discussing today. The issues are either regulatory or legislative in context and are described below.

### **Regulatory**

#### *Definition of post September 11<sup>th</sup> threat*

The terrorist attacks of September 11<sup>th</sup> certainly awakened the public to a previously unfathomable type of threat. Now, the general public opinion seems to be that anything, any type of threat, is conceivable, and everything possible should be done to safeguard against these threats. The nuclear industry is bearing a significant impact from this fear; however, as a commercial facility, how much should a plant reasonably be expected to defend against? There are a few key questions that are being debated as a part of this issue, all somewhat related to each other.

First, is a well-coordinated, large-scale attack of September 11<sup>th</sup> magnitude likely to occur at a nuclear power plant? The argument from the industry is that U.S. nuclear plants are among the

---

<sup>17</sup> Paul Leventhal, NCI. Prepared Witness Testimony to House Energy and Commerce Committee, December 5, 2001

most well defended and hardened facilities in the world, so there are much more attractive targets for a terrorist or other attacker. On the other hand, the environmental consequences of an attack that results in radiological release are potentially significant, so the motivation for an attacker is even greater. Even if there were no radiological release, the psychological consequences of an attack on a nuclear facility would be severe.

The second question is, if an attack were to occur, what are the chances that it would even cause a radiological leak? The standard security measures described in this report indicate how difficult it would be to breach security to the point of a causing a radiological release; however, the fact remains that reactor containment structures were not designed under consideration of a massive airplane impact. What would happen if another scenario, one that has never been thought of yet, occurs at a nuclear power plant? It is unreasonable to think that even the highest amount of safeguards and security measures will be capable of deterring every possible type of attack.

### *Re-evaluation of the DBT*

If it is impossible to protect against absolutely every threat, as the last section suggests, what level of defense is *reasonable*? Obviously, because of the potential damage risks, the low probability of a successful attack cannot be a justification for discounting the calls for an enhanced DBT. Since September 11<sup>th</sup>, re-evaluation of the DBT has been a major portion of the NRC's top-to-bottom security review and it is affecting nearly every other aspect of their decision-making with regards to security.

It is clear that the current DBT is less sophisticated than the September 11<sup>th</sup> attacks. The number of attackers in the DBT is much less than 19, for instance, and the DBT does not include airborne attack or the existence of more than one attacking team. Critics are calling the DBT “unrealistically small” and want it to include the possibility of a suicide attack, an increased number of separate, coordinated attacks, and an increased number of attackers with some with insider knowledge of plant characteristics.<sup>18</sup> On the other hand, automatically changing the DBT

---

<sup>18</sup> Behrens, Carl E. “Nuclear Powerplants: Vulnerability to Terrorist Attack.”

to a level as severe as September 11<sup>th</sup> without substantial analytic discussion would be careless. Unfortunately, there is no quantitative method of evaluating the adequacy of the DBT. The NRC is collaborating with the Federal Bureau of Investigations, Department of Energy, Department of Defense, and other key agencies to assess probabilities of various types of threats. This will have a significant bearing on any changes to the DBT. More importantly, though, these agencies are discussing where exactly the line should be drawn between licensee and government responsibility in protecting against the plausible threats. The DBT should represent the written agreement between the private and public sectors regarding this issue.

### *Force-on-Force testing*

After September 11<sup>th</sup>, the pilot SPA program and all ongoing OSRE force-on-force exercises were suspended indefinitely. Security forces were focused on other more urgent tasks, such as compliance with the ICM's, and any distraction from that work was deemed too dangerous.

The break in flow of the force-on-force testing programs has given extra wind to the critics of the SPA program, who have claimed since its inception that it gives too much control to industry as an attempt by the NRC to hide unsatisfactory OSRE records of the past. Critics such as Rep. Ed Markey (D-MA) point out that almost 50% (37 out of 81) of the OSRE exercises that were performed between 1991-2001 showed “significant vulnerabilities.”<sup>19</sup> On the other hand, the industry and the NRC explain that an OSRE is specifically intended to “test to failure,” thus results should be expected to show weaknesses.<sup>20</sup>

This report does not intend to analyze the adequacy of either the SPA or OSRE system. It is nevertheless important to note that the debate regarding force-on-force testing is closely tied to the overall top-to-bottom security review. Any change in the DBT will obviously affect the criteria used to evaluate a force-on-force test. The NRC is faced with the challenge of defending the adequacy of its current OSRE system when in all likelihood the system will have to be changed as soon as its re-evaluation of the DBT is complete.

---

<sup>19</sup> Markey, Rep. Edward J. Testimony to United States Senate Committee on Environment and Public Works. June 5, 2002.

<sup>20</sup> Hendricks, Lynnette. Personal interview. 6 June 2002.

### *Integration with national plans*

One of the keys to the effective security response discussed earlier was interagency coordination. The NRC has a central role in this coordination because of its role in threat assessment activities. Currently, there is not a unified system of threat response levels at the NRC that coincides with the other intelligence agencies and the Office of Homeland Security (OHS). While this is not purely a regulatory issue, it is certainly one that the NRC has undertaken as a priority of the new NSIR organization.

The OHS quickly created a five-level Homeland Security Advisory System, with the idea that all other security-related organizations would tailor their plans around the OHS guidelines for each level and integrate their own more detailed plans as necessary. The NRC has participated in recent industry workshops to follow this lead. There is some concern about where the “normal” level of nuclear plant security lies within the 5-level system. For example, the nuclear industry is worried that the NRC will set the new DBT so high that it would actually correspond to the elevated, or intermediate, OHS Advisory System level. This would mean that nuclear plants would be required at all times, even when the rest of the nation is at a low-risk (green) level, to be operating at heightened level of security.<sup>21</sup> The NRC generally takes the position of the industry, but there is considerable pressure from interest groups and some public officials who believe that the threat environment in the nuclear industry is uniquely more demanding than that of the rest of the nation’s critical infrastructure.

### *Other security risks*

Another issue in the regulatory domain right now is the adequacy of security for spent fuel pools, on-site dry cask storage, non-power reactors, and decommissioning plants. Many people who have voiced concerns to the NRC recently have been focused primarily on these subjects because they feel that the resistance to an attack at these places may be weaker than that associated with an operating reactor. Not only are critics worried about a direct physical assault on these sites,

---

<sup>21</sup> Doug Walters, NEI. Personal interview, June 18, 2002.

but also the potential for theft of the nuclear material located at these sites, which can be used in a radiological “dirty-bomb.”

While the validity of these arguments is still debatable, it is evident that the NRC needs to include reassessment of all aspects of its licensed facilities, not simply the operating reactor itself, in its security review. Any changes to the DBT or other regulatory measures need to incorporate the entire spectrum of possible targets.

## **Legislative**

### *Federalization of Security Workforce*

After September 11<sup>th</sup>, some legislators felt that the best way to ensure adequate security will be to make security forces a federal entity under command of the NRC. The Nuclear Security Act of 2001, Senate bill S.1746, proposed to give the NRC the responsibility of establishing and maintaining the security forces at each of its licensed facilities. As stated before, this is currently a responsibility of the licensees. S.1746 and a companion house bill, HR. 3382, contain some specific mandates on how the NRC should structure and manage the federal security force.

Those promoting federalization believe that having the forces under NRC control will give the federal government more authority to ensure security, for the same reason that airport security screeners were recently federalized in the Aviation and Transportation Security Act of 2001. Another reason why legislators have been interested in federalizing the workforce is the questionable results of OSRE testing in the past. On the other hand, critics of federalization, including the NRC, argue that comparison of the aviation and nuclear security systems is unfair to the nuclear industry because there is ample evidence that nuclear security forces are better regulated and more capable than private airport screeners were. They also argue that changing nuclear security from a private to federal responsibility will only disrupt the well-established, well-trained organization that is already in place. It would also divide the chain of command at the plant between the plant operating staff and the federal security force. The addition of security responsibilities to the NRC would nearly triple the size of the agency, in addition to

changing its focus from a primarily regulatory body to a defense agency. This would arguably weaken its regulatory authority and complicate its mission.<sup>22</sup>

S.1746, the proposed Nuclear Security Act of 2001, was amended in late July in the Senate Environment and Public Works committee to rescind the section on federalization of the security workforce. After 8 months of debate, it seems that the issue has calmed for the most part, and legislators are shifting focus towards other issues of nuclear security discussed below.

### *Provisions for Security Personnel*

The Atomic Energy Act of 1954 (AEA) permits security personnel at Department of Energy (DOE) facilities to carry arms, make arrests, and use necessary force as the DOE deems necessary for common defense. However, the type of weapons that commercial security guards at civilian NRC-licensed facilities are allowed to possess is the determination of state law. As a result, nuclear security guards from various plants have different types of weaponry, some more adequate than others. State law on the legal use of these weapons also differs. For example, some guards may be subject to state prosecution for an action taken during the course of their duty if it is not deemed to be for protection of a direct life threat.

On October 30, 2001, the United States Senate began consideration of a bill, S.1586, to address some of these concerns. The first key component of S.1586 would permit the NRC to authorize qualified security personnel to carry certain firearms during the course of their duty. The second would allow security personnel to make an arrest without a warrant of any individual threatening the security of an NRC licensed facility. The bill falls short of protecting guards against state persecution for firing a weapon in defense of plant security. Nevertheless, it is an important step toward improving the capabilities of security personnel.

S.1586 has not encountered serious criticism by any parties. Interest groups have not protested the bill, as it is generally agreed to be a positive improvement upon a longstanding legislative inequity. The nuclear industry has supported strengthening the authority of guard forces even

---

<sup>22</sup> “Implications of Security Force Federalization on Nuclear Power Plant Security.” p. 6.

before September 11<sup>th</sup>, but it was as a result of September 11<sup>th</sup> that the Congress became interested in prioritizing these security measures.

### *Control over the Design Basis Threat*

Historically the NRC has maintained the sole authority to set and monitor the DBT. However, after September 11<sup>th</sup>, members of Congress who are concerned with the issue have suggested legislation to mandate action by the NRC. Part of Congress's interest simply reflects homeland security concerns across the board, but a few members of Congress have expressed frustration with the NRC's response to September 11<sup>th</sup>. They claim that the agency's response has been too slow, or its attitude has been too casual. Regardless of the validity of these claims, Congress has been quick to step into the NRC's role. Amendment 12 to the Price-Anderson Reauthorization Act of 2001, of which both the House and Senate have passed independent versions, calls for a Presidential study to classify types of threats as federal or private responsibilities. The NRC would then make any necessary regulatory changes to take into account the licensee responsibilities determined by the study.

A more aggressive approach was included in S.1746, the Nuclear Security Act of 2001. It lists 10 specific threats, such as a September 11<sup>th</sup>-like attack, that must be included in the DBT. It also contains sections requiring revision every 3 years of the DBT by the Commission in consultation with the Office of Homeland Security, Department of Defense, the Attorney General, and other federal, state, and local agencies. Hiring, training, testing (OSRE), and appropriations are among the other aspects of the NRC's current responsibilities that are addressed.

When S.1746 was amended to rescind the proposal of federalization of security forces, the specific legislation regarding the DBT and OSRE system remained intact. The revised Nuclear Security Act of 2002 still contains prescriptive mandates for various changes to NRC oversight. While the effect of increased Congressional interest in the DBT is unclear, their steady interest in the matter is clearly evident.

## *Homeland Security*

The Department of Homeland Security (DHS) is currently the highest legislative priority. Critics of the Department worry that it will be difficult to fuse numerous large federal agencies without diffusing the main security goals; however, within the nuclear industry the responsibility of the Department is fairly limited since industry still maintains responsibility for day-to-day security operations. Creation of this new department is hoped to be a cornerstone for the nuclear industry to better incorporate all of its federal, state, and local resources into one unified security system.

Day-to-day physical security of nuclear facilities will be incorporated into one of the four major categories of the DHS, the Information Analysis and Infrastructure Protection division, through threat assessment and overall infrastructure protection strategies. In Spring 2002 the OHS held workshops with representatives of industry, the NRC, federal agencies, state and local governments, and other stakeholders to gain input on what these organizations need from the new Department. The near-term priority of the workgroups was the overarching National Physical Infrastructure Protection Plan strategy, which will inform fiscal year 2004-2006 goals. After that point, more specific integrated plans, including the energy plan, are expected by September of 2002.<sup>23</sup> In the end, it is expected that the DHS will take the lead in interagency collaboration and communication between intelligence communities, which are responsibilities less appropriate for the nuclear industry and the NRC.

Another of the four major categories in the DHS will be Emergency Preparedness and Response. One of 12 major initiatives in this organization is preparation for chemical, biological, radiological, and nuclear contamination. A radiological release due to attack on a commercial nuclear power plant would fall under this category. Under the President's proposal, the DHS would assume control of specialized emergency response agencies such as the Federal Emergency Management Agency (FEMA), currently the lead federal agency for nuclear power plant emergency response.

---

<sup>23</sup> Zimmerman, Roy. Personal Interview July 2, 2002.

Legislators across the board support the basic concept of President Bush’s Homeland Security Act. The debate at this time concerns the reorganization of certain agencies into the DHS. Many in Congress are questioning the need for FEMA and the Coast Guard, for instance, which primarily respond to natural disasters and non-homeland security crises, to be attached to the DHS. Senator Jim Jeffords (I-Vt) has said, “I am not advocating that FEMA not be a part of the new department. But I am advocating that FEMA remain a distinct entity within the department to help preserve its focus and mission.”<sup>24</sup>

---

<sup>24</sup> Jeffords, Sen. Jim. Opening statement to United States Senate Committee on Environment and Public Works. 10 July 2002.

## Recommendations to Relevant Agencies and Organizations

---

As stated before, this report is not intended to evaluate complicated technical analyses regarding the changes in the DBT or the force-on-force testing scheme. Much of this information is classified and out of the scope of this report; however, some general observations can be made about how these and other policy-related changes should be implemented. Role definition will be an important step towards appropriate policy implementation, so this section identifies some near and long term suggestions for relevant contributors to nuclear plant security.

### *Nuclear Regulatory Commission*

First, the NRC needs to act as quickly as possible to complete its review of the DBT and make a formal change, if necessary. It is obvious that the NRC is working hard on its top-to-bottom review, but the absence of any permanent solution is costly to the industry. Lance Terry, Senior Vice President and Principal Nuclear Officer at TXU Energy, has said that “the commission often spends too much time on interim compensatory measures rather than the comprehensive review.”<sup>25</sup> The primary focus of the NRC should be on long-term solutions, rather than interim solutions, now that the initial chaos from September 11<sup>th</sup> has subsided. Likewise, the evaluation of the OSRE system should be expedited once the new DBT is established. Because force-on-force exercises will have to be modified for the new DBT, the new exercises should be run as frequently as possible to uncover any potential problems with either the DBT or testing system.

A general recommendation to the NRC is that it consider its top-to-bottom security review as an ongoing assessment and not limited to responding to post-September 11<sup>th</sup> needs. Specifically, the NSIR organization within the NRC should be proactive in its threat assessment activities and continuously revisit the DBT. The agency should be open to utilizing the skills of other government agencies and intelligence sources to constantly review the adequacy of the Commission’s security policies. A collaborative and receptive philosophy is appropriate for the NRC now and in the future.

---

<sup>25</sup> Terry, Lance. Testimony to United States House of Representatives Energy and Commerce Committee, 11 April 2002.

## *Industry*

The licensees' main responsibility is to maintain solid performance of their security duties

While this may seem obvious, it is an essential key to maintaining public confidence and support.

Any event that draws attention to nuclear security would give detractors media time to spread misinformation about the industry, or giving Congress the incentive to pass unnecessary laws.

Steady performance in the wake of a tremendous event such as September 11<sup>th</sup> is an indication of the reliability of nuclear plant security before and after the event.

The final recommendation to licensees is that they take initiative to foster stronger relationships

with state and local resources. It is hoped that the DHS will facilitate better collaboration on a federal level, but licensees need to make sure there is adequate cooperation on the state and local ends. The emergency response plans to which licensees are responsible depend on smooth collaboration of multiple outside resources. Licensees do a good job of formulating their plans, but more emphasis should be placed on implementation of the plans. State and local responsibility within this context is elaborated below.

## *State and Local Authorities*

State and local agencies should also take initiative to foster stronger relationships with licensees.

The overriding responsibility of state and local governments in the entire security scheme is mitigation, or emergency response. In the unlikely event of an actual emergency, state and local responders will be the first on the scene. Besides some obvious national-level tasks, "local leaders closer to the problem are going to do a better job of developing ways to prevent and respond to attacks than Washington bureaucrats."<sup>26</sup> Homeland security planning in each state should provide their plants with specific information about how they will contribute to an emergency response effort. This should go beyond saying what resources are available. It is more important for the plants to know when, and under what circumstances, the state and local governments will commit to certain levels of involvement. This is essential to plants for

---

<sup>26</sup> McIntyre, Dave. "Waiting for Godot's Strategy."

formulating their own response plans in coordination with outside resources and will help them make important, timely decisions in emergency situations.

In addition, intelligence and emergency response agencies should maximize their efforts by integrating homeland security resources across a variety of industries or emergency situations.

As an example, many state and local authorities since September 11<sup>th</sup> have considered purchasing large quantities of potassium iodide (KI) pills for emergency purposes in areas near the plants. These governments should be aware that KI pills only defend the thyroid gland against radioactive iodine, a single, well-defined radiological threat. They should be careful not to place too much emphasis on KI distribution in their mitigation plans, because evacuation or sheltering is the only true defense for the entire body. State and local funding for emergency response might be more effective if applied to evacuation training, which can apply to natural disasters or other industrial accidents. Nevertheless, state and local emergency response organizations need to develop plans for distribution of the potassium iodide. Currently FEMA is responsible for distributing pills and organizing evacuation or other response efforts outside a 10-mile radius of the plant. Early efforts by state and local governments to collaborate with FEMA will prevent confusion of responsibilities or lack of organization in critical situations.

#### *Office/Department of Homeland Security*

Homeland Security is an extremely complex issue in the public policy forum. It is unavoidably scattered across many issues, industries, levels of government, and so on. In order to simplify this report, only some very specific recommendations that relate directly to nuclear energy interests will be addressed.

The first recommendation is that the DHS use its organizational capabilities as an assessment tool rather than try to get directly involved in specific decision-making activities. It should assess the strengths and weaknesses of licensees, the NRC, and various levels of government and suggest ways of eliminating weaknesses or overlapping roles. This utilizes the DHS's strong organizational resources without displacing the resources of those parties who have the most experience and expertise.

Building on this idea, the DHS should apply the nation's broad homeland security objectives to prioritization of the needs of the Department in the near and long term. Arguably one of the most difficult tasks for the DHS will be deciding how to allocate a limited amount of funds and resources.<sup>27</sup> With this in mind, it will be important for those in decision-making positions to understand that the nuclear industry already has one of the most heavily regulated and well-developed security systems. In comparison, other industries of similar risk-status, such as chemical and biological facilities, lack the standards already in place at nuclear facilities yet are still under-emphasized in homeland security agendas.<sup>28</sup> Thus, the potential benefits of allocating a certain level of funding to these industries are likely much greater than the benefits one would see at a nuclear facility.

The DHS should take extreme care not to overshadow the other non-homeland security related responsibilities of FEMA and the other federal agencies it may take over in the future. The Department does have the capability of integrating all 22 agencies in a comprehensive homeland security effort, but the other obligations of these agencies must not be forgotten. There have been many suggestions from Congress on exactly how this might be accomplished. Departments within FEMA should be separated based on homeland security and non-homeland security duties. The DHS should provide some level of autonomy for these agencies to carry out their normal peacetime duties, but if a nuclear incident were to occur, the DHS would then take control of FEMA.

Finally, the OHS should continue the practice as mediator of a multi-agency, multi-government workgroup. To emphasize, the OHS should be a *mediator*--someone without direct investment in the security operations. Also, the workgroup should be an ongoing *proactive* group, meeting regularly and discussing important security issues on the forefront. This group should pull representatives from every relevant party. A main goal of this workgroup should be to establish clear interagency and intergovernmental command and control structure and foster professional, dependable relationships. As it stands, the Office of Homeland Security seems best fitted for this

---

<sup>27</sup> Protecting the American Homeland: A Preliminary Analysis. Brookings Institution Press. p. 78.

<sup>28</sup> Washington Post, "U.S. Faulted on Chemical Plants' Security." Eric Pianin, June 13, 2002

role. First, at the Cabinet level position it has the potential ability to oversee every relevant party that would be involved. Second, it has the organizational structure to excel in bring multiple resources together. If these workgroups are developed for all the other critical infrastructure industries, the OHS will be able to specialize their skills in leading such groups. In the end, this will benefit both the OHS and the critical infrastructure industries.

### *Federal Agencies*

If there is one lesson-learned from the events of September 11<sup>th</sup>, it should be that interagency coordination and communication are essential to both prevention and mitigation in emergency situations. As explained above, the Department of Homeland Security should address this concern. Above and beyond this, a few key agencies warrant specific mention in this section.

Along with the NRC and the DHS, the Department of Defense should participate in serious discussions with the industry to identify the conditions for intervention and then develop collaborative response plans. According to 10 CFR 50.13, a licensee is not responsible to protect against the effects of an “enemy of state” attack. Obviously, responsibility for this would fall to the federal government, but for the most part there are no clear written policies on how government agencies are expected to protect against specific types of threat to a commercial nuclear facility. As the previous section, “Keys to Effective Security Program,” explains, specific written procedures for action are absolutely essential.

The newly formed Transportation Security Agency (TSA) and the Federal Aviation Administration should take steps to prevent against the threat of an aircraft attack on a nuclear power plant. In the ongoing debate about possibility of this situation, the industry has taken the majority of the blame for not being prepared to defend an air attack, even though it is generally considered to be an “enemy of state” attack. NRC Chairman Richard Meserve has stated that “the nation’s efforts associated with protecting against terrorist attacks by air should be directed toward enhancing security at airports and within airplanes, and not toward seeking to defend all potential targets of such terrorism.”<sup>29</sup> The federal government has acknowledged this need through passage of the Aviation and Transportation Security Act of 2001. This act federalized

---

<sup>29</sup> Meserve, Richard. Letter to Sen. James Jeffords, 17 December 2001. p. 9

screening personnel at all airports and created the TSA as a new agency under the Department of Transportation. A potential benefit of the TSA is that it can protect against airborne attacks on all types of facilities at the “front end,”<sup>30</sup> which is much more efficient than having each individual private owner attempt its own protection schemes.

### *Congress*

Members of Congress should be careful not let their eagerness to improve homeland security translate into overzealous decisions regarding specific nuclear power plant security legislation.

The enthusiasm of some members in promoting federalization of the security workforce is an example of this situation. This legislation would result in serious disruptions of the security framework simply for the sake of appeasing post-September 11<sup>th</sup> fears through government action. Debate over federalization in the past eight months has been substantial, but other more important concerns have taken priority. Congress is focusing now on how to strengthen independent nuclear security forces in other ways more congruent with the overall national homeland security agenda.

One way of accomplishing this is to pass the legislation to enhance the ability of a private security guard to perform his duties. S.1586 is a positive step towards strengthening security without federalization and therefore should be enacted. While state laws are an important check to the legislative process, a uniform standard will provide the congruence necessary to ensure adequate protection at each and every site. Federal protection, rather than ownership, of the guard forces is a more balanced approach overall.

Likewise, balance between legislative and regulatory authority is needed in the development of the new DBT. Understandably, Congress wants to become more involved in protecting homeland security on all fronts, but its collective level of expertise is much lower than the NRC's. Rather than mandate a specific type of change to the DBT, as the Nuclear Security Act suggests, Congress should simply encourage more effective collaboration between the NRC, industry, and government parties. For instance, the Presidential review suggested in the Price-

---

<sup>30</sup> i.e., as passengers board an aircraft

Anderson amendment will “avoid having regulatory and security decisions made in a political vacuum without necessary guidance from government experts in the areas of security and intelligence gathering.”<sup>31</sup> In general, Congress needs to maintain a balanced approach to security decisions in the future. It should appropriately critique the NRC and industry when necessary, but also be cautious of overstepping its boundaries and assuming responsibilities best left to other parties.

---

<sup>31</sup> Benjamin, Jeff. Testimony to the United States House of Representatives Committee on Energy and Commerce, 5 December 2001.

## Conclusions

---

The nuclear power industry has one of the most well protected commercial security systems in the United States. However, as the saying goes, there is always room for improvement. September 11<sup>th</sup> only highlighted the need for continuous re-evaluation of security policies, especially in light of the ever-changing threat environment.

At this time, any action regarding nuclear security should take into consideration the national homeland security initiative. Prioritization will be important to the success of government programs relating to homeland security. Other physical infrastructures with the same risks as a nuclear facility include dams, chemical plants, electrical grids, water sources, oil and gas lines, and so on. Government agencies, through the lead of the DHS, should use the same criteria for security of all these commercial resources. This approach will lend itself towards efficiency and collaboration of government resources.

Federal, state, and local governments have a difficult role in security of commercial resources, because while they are in the private domain, they also potentially endanger a large portion of the general public. The “fair” lines of responsibility are anything but clear, so it makes sense to assign responsibility based on the most effective use of existing resources.

Intelligence gathering and terrorist prevention matters should remain a responsibility of federal, state, and local agencies that specialize in these areas. These agencies can consolidate their efforts towards all elements of homeland security, not just the nuclear industry. Day-to-day, on-site security operations should be the responsibility of the industry. The licensee has a vested interest in protecting its plant and has the most knowledge of plant details that are important to security. At the same time, it should be clear that a licensee cannot reasonably be expected to protect against large-scale “enemy of state” attacks. No commercial industry has the capability to do this. Federal regulation, i.e. the DBT, should be the line of division between government and licensee responsibilities. All parties play a role in event mitigation, although state and local emergency response agencies have the most critical task.

In general, these are the ideal responsibilities of each party. Obviously, however, the system is much more complicated than this. There will always be overlap of activities and responsibilities. And there will always be the possibility of a threat that simply cannot be prepared for despite all efforts. In the end, every level of government and the private sector needs to contribute their best resources and work together, through organization and communication, to ensuring adequate security commercial nuclear power plants.

## Appendix A: Glossary of Acronyms

---

CFR	Code of Federal Regulation
DBT	Design Basis Threat
DHS	Department of Homeland Security
DOE	Department of Energy
EPZ	Emergency Planning Zone
FEMA	Federal Emergency Management Agency
ICM	Interim Compensatory Measure
KI	Potassium Iodide
NEI	Nuclear Energy Institute
NRC	Nuclear Regulatory Commission
NSIR	Nuclear Security and Incident Response
OHS	Office of Homeland Security
OSRE	Operational Safety and Response Evaluation
SPA	Safeguards Performance Assessment
TSA	Transportation Security Agency

## Citations

---

Behrens, Carl E. "Nuclear Powerplants: Vulnerability to Terrorist Attack." Congressional Research Service Report for Congress, 1 March 2002.

Benjamin, Jeff. Testimony to the United States House of Representatives Committee on Energy and Commerce, 5 December 2001.

"Emergency Preparedness Near Nuclear Power Plants." Nuclear Energy Institute Fact Sheet. <<http://www.nei.org/doc.asp?catnum=3&catid=49>>. [February 2002].

Hendricks, Lynnette. Nuclear Energy Institute. Personal Interview, 6 June 2002.

"Implications of Security Force Federalization on Nuclear Power Plant Security." An Evaluation by the Nuclear Energy Institute, December 2001.

Jeffords, Sen. James. Opening statement to United States Senate Committee on Environment and Public Works. 10 July 2002.

Leventhal, Paul. Nuclear Control Institute. Prepared Witness Testimony to the House Energy and Commerce Committee, 5 December 2001.

McIntyre, Dave. "Waiting for Godot's Strategy." Anser Institute for Homeland Security, May 2002. <<http://www.homelandsecurity.org>>.

Markey, Rep. Edward J. Testimony to United States Senate Committee on Environment and Public Works. June 5, 2002.

Meserve, Richard. Letter to Sen. James Jeffords, 17 December 2001. <[http://member.nei.org/documents/communications\\_resources/acrobat/NEING1220012728.pdf](http://member.nei.org/documents/communications_resources/acrobat/NEING1220012728.pdf)>.

Office of Management and Budget. *Annual Report to Congress on Combating Terrorism*, August 2001. <[www.whitehouse.gov/omb/legislative/nsd\\_annual\\_report2001.pdf](http://www.whitehouse.gov/omb/legislative/nsd_annual_report2001.pdf)>.

Pianin, Eric. "U.S. Faulted on Chemical Plants' Security." *Washington Post*. Page A10, 13 June 2002.

Protecting the American Homeland: A Preliminary Analysis. Washington DC: Brookings Institution Press, 2002.

Stephan, Bob. Office of Homeland Security. Personal interview, 4 June 2002.

Terry, Lance. Testimony to United States House of Representatives Energy and Commerce Committee, 11 April 2002.

Walters, Doug. Nuclear Energy Institute. Personal interview, 18 June 2002.

Yim, Randall A. "National Preparedness: Integration of Federal, State, Local, and Private Sector Efforts Is Critical to an Effective National Strategy for Homeland Security." GAO-02-621T, 11 April 2002.

Zimmerman, Roy. Nuclear Regulatory Commission. Personal Interview July 2, 2002.