

**Marvin Fertel
Senior Vice President and Chief Nuclear Officer
Nuclear Energy Institute**

**Written Testimony
U.S. Senate
Committee on Environment and Public Works
Subcommittee on Clear Air and Nuclear Safety**

**Washington, D.C.
February 28, 2008**

Chairman Carper, ranking member George Voinovich, and distinguished members of the subcommittee, I am Marvin Fertel, Executive Vice President and Chief Nuclear Officer at the Nuclear Energy Institute (NEI). I am honored to address the subcommittee on the subject of "Security of Our Nation's Nuclear Plants."

NEI brings together and is responsible for developing policy for the U.S. nuclear industry. NEI's 270 corporate and other members represent a broad spectrum of interests, including every U.S. electric company that operates a nuclear power plant. NEI's membership also includes nuclear fuel cycle companies, suppliers, engineering and consulting firms, national research laboratories, manufacturers of radiopharmaceuticals, universities, labor unions, and law firms.

I am here to discuss nuclear security at the nation's 104 commercial nuclear power plants at 65 separate sites in 31 states. These plants are responsible for producing 20 percent of the electricity in the United States. In particular, I will also discuss the industry response to an issue we take very seriously – security officer inattentiveness. This is an issue that has gotten attention recently because of an incident at the Peach Bottom nuclear power station. The nuclear industry as a whole is proud of its safety and security programs and their records. We put great stock in and value each of the security professionals that work day in and day out to protect our employees that work at the plant, and the public that lives around the plants and the power plant itself. Yet, inattentiveness by even one individual does not meet our expectations and the situation that creates the inattentiveness needs to be corrected. We need to understand and deal with the individual and the specific situation appropriately. But, more importantly, we must better understand any conditions that might contribute to inattentiveness and mitigate them across the industry

My testimony will address the following issues:

- Security at the nation's 65 commercial nuclear power plants. America's commercial nuclear power plants have long been the most secure facilities in our nation's critical infrastructure. Even so, we have made huge changes since the September 11 terrorist attacks and they are considerably more secure today.

- The aggressive actions the nuclear industry has taken in response to security officer inattentiveness incidents particularly following the situation at Peach Bottom.
- The use of Wackenhut Special Operations as the contractor to support the industry composite adversary force. Because the officers involved in the recent inattentiveness event were provided by Wackenhut, some have again raised concerns about the use of Wackenhut to manage the industry composite adversary force – the teams we use to test our security in exercises we call “Force-On-Force” (FOF).

Security At Our Facilities

Unique among the nations critical infrastructure, nuclear plants have, even prior to 9/11 had to meet security requirements required by the U.S. Nuclear Regulatory Commission (NRC). Following the September 2001 attacks, the NRC has increased nuclear facility security requirements numerous times by issuing orders and other formal requirements, and is now in the process of codifying additional requirements in rulemakings.

Since 9/11 the industry has invested more than \$2 billion in additional security at nuclear plant sites and has increased the number of specially trained, well-armed security forces by more than 60 percent. These officers are better trained, better equipped and armed, better led and better supported with stronger protective systems and barriers, and better tested and evaluated by the industry and independently by the NRC.

The industry is proud of its security programs and the example they provide for other sectors of America’s critical industrial infrastructure. I urge members of this subcommittee and any member of Congress visit a nuclear plant to see these security programs firsthand and meet the professionals that manage and implement our security programs. All U.S. nuclear plants must meet the same high standards established and inspected by the NRC.

Compared to other commercial facilities, nuclear power plants start with a clear advantage in the area of security. The structures that house reactors and critical systems are built to withstand natural events such as earthquakes, hurricanes, tornadoes, fires and floods. They are massive structures with thick, steel-reinforced exterior walls and internal barriers of reinforced concrete. As such, the structures provide a large measure of protection against potential attacks. In addition, the “defense-in-depth” philosophy used in nuclear facility design means that plants have redundant systems to ensure safety. Many of these redundant safety systems are separated physically so that if one area of the plant is compromised, backup systems in another part of the plant can maintain safety. This redundancy provides a capability to withstand securely and safely a variety of events, natural or man-made.

The difficult-to-penetrate structures are just the first level of a multistage, integrated security strategy. Nuclear power plant security is designed with concentric perimeters with increased security at each level. Physical barriers protect against unauthorized personnel and vehicle intrusion, including truck bombs. These security zones are protected by trained and armed professionals, who use hardened defensive fighting positions located throughout the plant, if needed. In the innermost security zone, access to the vital areas of our plants is strictly controlled using biometrics and other technologies. Critical areas are constantly surveilled and monitored using state-of-the-art detection equipment. Strict access control is maintained using biometrics and other technologies. Industry employees with unescorted access are subject to a systematic fitness-for-duty program and a continual behavioral observation program and must undergo comprehensive background checks.

Every plant has extensive plans and arrangements with state and local law enforcement and emergency response entities. In addition, every plant must conduct drills and exercises to ensure a well-prepared, comprehensive emergency response plan.

This combination of strong structures, perimeter protection, access controls and other security measures greatly exceeds the security provided for other elements of the America's critical infrastructure.

One of the security standards mandated by the NRC is the "design basis threat" (DBT). The DBT provides the characteristics and capabilities of a potential attacking force – in effect, the threat each site must be able to defend against under any conditions. Every site tests its security forces against this standard and the NRC inspects against it at mandated FOF exercises. No other sector of the civilian operated critical infrastructure has a defined DBT.

Certainly the industry recognizes – as does the NRC and U.S. Department of Homeland Security (DHS) – that it is possible that there could be threats to our plants greater than or less than what is defined by the DBT. Based upon tabletop exercises done at all sites and additional simulations done at some sites, we would expect to be successful against most credible threats even at higher levels. But with any fixed size protective force and the inherent limitations of a private sector entity, on intelligence gathering, deadly force capabilities and authorities, there is a limit to its capability by itself. Against a much larger force, plant paramilitary security forces would certainly offer a significant degree of deterrence and a strong initial defense. But at some point such threats are the responsibility of the federal government, which has full intelligence, interdiction and military response capabilities. Since September 11, 2001, DHS, NRC, and the industry have recognized the importance of coordinating federal, state and local authorities with the industry to best defend against such an attack. The DHS, NRC and the industry established a program to integrate the response planning around nuclear plant sites. The mechanism for this planning was called "Comprehensive Review" and brought together the full potential of local, state and federal capability. Last year these

Comprehensive Reviews were completed for every site – well ahead of all other industrial sectors. The industry continues to work with DHS, FBI, NRC and other federal, state, and local law enforcement agencies to enhance the integrated response of all entities in the event of an attack at a nuclear power plant.

After 9/11, the NRC issued orders requiring sites to evaluate the impacts of losses of large areas of the plant due to fires and explosions. Each site conducted specific analyses to assess the implications of the requirements and identified “mitigation strategies” to address the results of the analyses. NRC independently reviewed the analyses and mitigating strategies. All sites have complied with the order and NRC is conducting inspections to ensure these strategies are now in place.

The improvements to an already robust security program since 9/11 have been broad-based and go far beyond the large increase of officers from 5,000 to 8,000. We now maintain a professional force of an average of 125 officers per site. We couple this professional force with better weapons, solid planning and tactics, effective training and exercises, strong barriers and the latest in defensive and surveillance technology all deployed with strong security designs in a naturally hard facility. Other changes include physical improvements to provide additional protection against vehicle bombs as well as additional protective measures against water- and land-based assaults. Every plant has increased security patrols, augmented security forces, added more security posts, increased vehicle standoff distances, tightened access controls, and enhanced coordination with state and local law enforcement. This then is all backed up and integrated with competent, trained local, state and federal capabilities.

Security Officer Attentiveness

In this environment of strong security and professionalism, there has arisen recently an issue of security officer attentiveness while on duty. This is not really an issue of training. Our officers typically receive 160 hours of initial training and 120 hours of recurring training each year. Nor is it necessarily an issue of fatigue given the current and new workhour limitations required by the NRC.

Our security officers face many challenges in discharging their responsibility of protecting the nation’s 104 operating nuclear power plants 24 hours a day, seven days a week. Every company expects the on duty security force to be attentive and able to respond when called upon. However, it is important to recognize that while there were 12 incidents of inattentive officers during 2007, security officers spent approximately 16 million man-hours on duty. Most of the time, the work is tedious and boring. Nevertheless, inattentiveness is unacceptable behavior. We need to correct it at the individual level, at the plant level and remove or mitigate the root causes. The potential for inattentiveness is not uniquely a contract security officer matter, it is a human being matter that requires the articulation of appropriate expectations to the security officers, appropriate involvement by supervision and management and a

culture that fosters professionalism, openness, and appropriate reactions to conditions or situations that result in attentiveness.

Following the Peach Bottom situation, NEI communicated with the industry Chief Nuclear Officers (CNOs) and recommended several immediate actions be taken by each site. Specifically, we recommended more frequent checks of the security post positions by security supervisors, more frequent communication with those posts, rotating the officers in those posts more frequently, more observation of activities in the ready rooms and ensuring the environmental conditions in these areas are conducive to officer attentiveness. For example, if there is heating and cooling inside the room or bullet resistant enclosure, the site should make certain it is working properly to ensure officers remain alert.

We also emphasized the need for leadership at the site and encouraged each CNO to meet with the security organization to discuss the importance of officers being attentive to their duties and reinforce the organizational expectations and standards

The industry also created a task force which is actively engaged examining security organization cultural issues as well as additional measures that may be effective for ensuring security officer attentiveness.

The task force immediately developed two documents focused on the attentiveness issue. One document is a shift briefing paper that reinforces the security officer's roles and responsibilities for identifying and reporting of inattentiveness and other inappropriate behavior.

The second document is a security post evaluation checklist that is a structured review of each security post on site. This process serves to identify if the environment promotes attentiveness and if not, provides attentiveness aides for consideration.

We recognize that these are in part procedural adjustments that may not get to the core of the matter. Over the next few months, the task force is working to define the performance and professional standards needed to promote the security culture desired across all of our plants. This will include consideration of appropriate policy for addressing incidents where inattentiveness occurs.

It is important to recognize that the leadership at nuclear power plants expects an extremely high standard of professionalism, accountability and performance from all personnel that work at the plant. In this regard, all of the sites have processes in place to foster and support the desired culture.

Leadership at every company and every site expects and advocates a Safety Conscious Work Environment (SCWE) program which is designed to ensure individuals feel free to raise concerns and are confident those concerns will be promptly reviewed and resolved

with a priority appropriate to their significance. Security officers, just like all other personnel on the site, are therefore encouraged and expected to promptly report concerns and issues to supervision for resolution under one or more existing plant programs. These programs include the Corrective Action Program, Employee Concerns Program, Access Authorization, Fitness-for-Duty, and Human Resources. Alternatively, the individual may report directly to any of these programs or to the NRC.

All nuclear power plant sites have Behavioral Observation Programs (BOP) designed to make all employees with unescorted access aware of their responsibilities to recognize individual behavior which, if left unattended, could lead to acts detrimental to public or site personnel health and safety. A key objective of the program is the recognition of behavior that is adverse to safety and security of the facility, including an unusual interest in or predisposition towards security and/or involvement in operations activities outside the normal work activities scope.

On a monthly basis, supervision/management formally documents that BOP monitoring has occurred. An annual review is performed and documented by supervision which typically includes behavior deviations reported to or observed by the supervisor. The supervisory review is evaluated by an Access Authorization program reviewing official to determine if additional action is required concerning the individual's trustworthiness, reliability and Fitness-for-Duty.

Force-on-Force Exercises And The Industry Composite Adversary Force

The industry has not only greatly improved its physical and operational security, but has also significantly improved the testing of that security.

Prior to the tragic events of September 11, 2001, NRC evaluated FOF exercises occurred roughly once every eight years at each site and there were no NRC requirements for annual exercises to be conducted at every site. Also, the pre-9/11 program did not have specific performance requirements for the adversary force that participated in the evaluated exercises.

Since 2004, each plant is required to conduct FOF testing of its security several times each year, with each security shift being tested every year as well as each site conducting an annual FOF exercise.

NRC conducts annual baseline inspections to validate the effectiveness of the overall site security training program, physical security efficiency and FOF exercises.

The Energy Policy Act of 2005 also mandates that one of these large-scale FOF exercises be formally evaluated by the NRC every three years. In 2007 we completed the first three-year cycle of NRC evaluated FOF security exercises – at every plant.

The NRC has also established standards for the qualifications of the adversary forces that participate in the FOF drills. While, the primary purpose of the FOF exercise is to test the defensive capabilities of the plant, an effective exercise obviously requires high performance by the adversary. Recognizing that the sites would be conducting as many as 15 drills and exercises in a three year period, the industry decided that there was value in establishing a process by which site personnel could gain expertise in performing as adversaries. To this end, the industry has established a Composite Adversary Force that is skilled in offensive tactics and has the training and qualifications to meet the NRC standard. This force consists of full-time, highly trained, security experts. The adversary team members are thoroughly trained, meet physical fitness requirements and demonstrate weapons proficiency to standards, including expertise in the use of state-of-the-art MILES laser based weaponry. The adversary force is used in the triennial NRC-evaluated exercises and thus presents a state-of-the-art challenge to the plants. In addition to evaluating the defensive capabilities of the plant, the NRC also evaluates the adversary force to ensure a robust exercise. Through this program, assurance is further provided that our security forces can successfully respond to a dedicated adversary team.

We are unaware of any security forces for any private industry that are subjected to such rigorous testing that includes FOF drills using a full-time dedicated team.

The Composite Adversary Force is managed under a contract with Wackenhut Special Operations Group. The management team is comprised of five individuals all of which have extensive special operations experience. The rest of the adversary team consists of individuals from power plant sites that are trained to meet the NRC standards and perform as part of the team for a period of between 12 and 18 months after which they return to their site to train and participate in FOF exercises. While some of the team members come from sites supported by Wackenhut, more than 50 percent do not come from Wackenhut sites. Regardless of whether the adversary forces themselves consist of personnel from Wackenhut or any other entity, they must perform to the standard that the NRC has established.

To further ensure the integrity of the exercises, employees recruited from plant sites are not permitted to participate in FOF exercises at their own plant. Also, team leaders who may have assessed security at plants in previous positions will not be team leaders for the FOF drills at those plants.

In any case, it is important to recognize that only the NRC evaluates the exercise including assessing the performance of the adversary force as well as the plant's defensive response.

By all accounts, the Composite Adversary Force's performance in the first three-year cycle has been exemplary and they are meeting or exceeding both NRC and industry expectations.

In summary, our defenses were robust prior to September 11, 2001 and they are significantly better today. It is highly unlikely that attackers could successfully breach security at a nuclear power plant and even more unlikely they could produce a release of radiation that would endanger the residents near the plant. We take security officer inattentiveness seriously. We have taken and are continuing to take aggressive action to ensure appropriate measures are in place. In addition, security at our nuclear power plants is not static. We are constantly reviewing and reevaluating our security programs. Consequently, America's nuclear energy industry will continue to play its role as a leader and model for protecting our country's critical infrastructure.