RulemakingComments Resource

From: cnelson66@aol.com
Sent: Thursday, June 06, 2013 9:47 AM
To: RulemakingComments Resource
Subject: Fwd: Undeliverable: Re: Access Disputes commnets
Attachments: Attachment; 911NRCReleasesecurity-enhancements.pdf; IndustrymeetsDBTChangedeadline102904.doc; lu66NRCCOMMENTS_-_CN.docx; NEIPlantSecurityReporttoCongress091404.pdf

-----Original Message-----
From: postmaster <postmaster@nrc.gov>
To: Cnelson66 <Cnelson66@aol.com>
Sent: Wed, Jun 5, 2013 12:02 pm
Subject: Undeliverable: Re: Access Disputes commnets

Delivery has failed to these recipients or distribution lists:

Rulemaking.Commnets@nrc.gov
The recipient's e-mail address was not found in the recipient's e-mail system. Microsoft Exchange will not try to redeliver this message for you. Please check the e-mail address and try resending this message, or provide the following diagnostic text to your system administrator.

Sent by Microsoft Exchange Server 2007

Diagnostic information for administrators:
Generating server: nrc.gov
Rulemaking.Commnets@nrc.gov
#550 5.1.1 RESOLVER.ADR.RecipNotFound; not found ##
Original message headers:

```
Received: from mail1.nrc.gov (148.184.176.41) by OWMS01.nrc.gov
 (148.184.100.43) with Microsoft SMTP Server id 8.3.298.1; Wed, 5 Jun 2013
 12:30:15 -0400
Received-SPF: Pass (mail1.nrc.gov: domain of Cnelson66@aol.com
  designates 64.12.143.82 as permitted sender)
  identity=mailfrom; client-ip=64.12.143.82;
  receiver=mail1.nrc.gov; envelope-from="Cnelson66@aol.com";
  x-sender="Cnelson66@aol.com"; x-conformance=spf_only;
  x-record-type="v=spf1"
Received-SPF: None (mail1.nrc.gov: no sender authenticity
  information available from domain of
  postmaster@omr-m09.mx.aol.com) identity=helo;
  client-ip=64.12.143.82; receiver=mail1.nrc.gov;
  envelope-from="Cnelson66@aol.com";
  x-sender="postmaster@omr-m09.mx.aol.com";
  x-conformance=spf_only
X-Ironport-ID: mail1
X-SBRS: 5.5
X-MID: 22188910
X-fn: 911NRCReleasesecurity-enhancements.pdf,
 IndustrymeetsDBTChangedeadline102904.doc, lu66NRCCOMMENTS - CN.docx,
 NEIPlantSecurityReporttoCongress091404.pdf
X-IronPort-AV: E=Sophos;i="4.87,808,1363147200";
```

d="xml'?docx'72,48?scan'72,48,208,217,32,72,48?rels'72,48,208,217,32,72,48?doc'72,48,208,217,32,72,48,32?pdf'72,48,208,217,32,72,48,32";a="22188910"
Received: from omr-m09.mx.aol.com ([64.12.143.82]) by mail1.nrc.gov with ESMTP; 05 Jun 2013 12:30:13 -0400
Received: from mtaomg-mb02.r1000.mx.aol.com (mtaomg-mb02.r1000.mx.aol.com [172.29.41.73]) by omr-m09.mx.aol.com (Outbound Mail Relay) with ESMTP id EFACA7000009B for <Rulemaking.Commnets@nrc.gov>; Wed, 5 Jun 2013 12:30:12 -0400 (EDT)
Received: from core-dhd003c.r1000.mail.aol.com (core-dhd003.r1000.mail.aol.com [172.29.209.131]) by mtaomg-mb02.r1000.mx.aol.com (OMAG/Core Interface) with ESMTP id E9F01E00008F for <Rulemaking.Commnets@nrc.gov>; Wed, 5 Jun 2013 12:30:11 -0400 (EDT)
From: <Cnelson66@aol.com>
Full-name: Cnelson66
Message-ID: <b5f11.4c9615bc.3ee0c193@aol.com>
Date: Wed, 5 Jun 2013 12:30:11 -0400
Subject: Re: Access Disputes commnets
To: <Rulemaking.Commnets@nrc.gov>
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="part1_b5f11.4c9615bc.3ee0c193_boundary"
X-Mailer: AOL 9.6 sub 168
X-Originating-IP: [99.50.247.146]
x-aol-global-disposition: G
X-AOL-VSS-INFO: 5400.1158/91213
X-AOL-VSS-CODE: clean
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=mx.aol.com;
s=20121107; t=1370449812;
bh=ci58Sbk4X3pGWxdWX8KX+a7Ve1yevY1YYSNDEgHvpJY=;
h=From:To:Subject:Message-ID:Date:MIME-Version:Content-Type;
b=DT0GwW49BHthrYsIMszBYwvE3HH7Ew1lS0Q1gm3dk+egonteQpSuhIcik1FUVn0lK
PQ2Snn90nZBVuKJjQsKmLjZchnYO/U/Lw945yUJ4IMYX6BFsHi3JpQFK/5HEZX9Y46
hnYuhshb/dC00g21XADJa094h/+o9gHV3rEt+wc4=
X-AOL-SCOLL-SCORE: 0:2:349384928:93952408
X-AOL-SCOLL-URL_COUNT: 0
x-aol-sid: 3039ac1d294951af679323e5
Return-Path: Cnelson66@aol.com

Attached Message

From:	Cnelson66@aol.com
To:	Rulemaking.Commnets@nrc.gov
Subject:	Re: Access Disputes commnets
Date:	Wed, 5 Jun 2013 12:30:11 -0400

Dear Ms. Vietti-Cook,

Please see the attached.

Thanks,

Charlie Nelson, Business Representative
I.B.E.W. Local Union #66

June 5, 2013

Ms. Annette L. Vietti-Cook
Secretary of the Commission
U.S. Nuclear Regulatory Commission
Washington, DC 20555-001

RE: Docket ID NRC-2013-0024, PRM 73-16

Dear Ms. Vietti-Cook:

My name is Charlie Nelson. I am the Business Representative of the International Brotherhood of Electrical Workers, AFL-CIO, Local Union 66, headquartered in Pasadena, Texas. My Local Union has an electric jurisdiction that spreads across the southern and mid region of Texas, including the South Texas Project Nuclear Operating Plants. Of my 3000 members, 300 work directly at this facility utilizing unescorted access working at the station on a daily basis.

The collective bargaining agreement has a binding arbitration procedure which has been used for discipline related matters over the years up to and including the unilateral removal of unescorted access. Losing unescorted access unilaterally in this industry is a dire situation to the employee. The damage to those workers who lose unescorted access is twofold: they lose their jobs without adequate recourse, and they immediately become ineligible to seek similar employment in the nuclear industry where unescorted access is required. It is a critical need to have this remedy avenue available to an employment dispute procedure. If this petition is enacted the only recourse left will be the reliance on a "management access review team" or cause the employee to seek whistleblowing activity, NRC ADR, or submit to OSHA.

At my represented facility, we have had several occasions of employees negatively impacted by overzealous decision makers in the security/access management process that required third party resolution. A Local Union has a duty to fairly represent employees, a legally defined duty I take very seriously on every occasion.

I and the Local 66 membership serving in the nuclear industry strongly oppose the industry's most recent attempt to circumvent the use of third party resolution by amending 10CFR73.56 to eliminate this method to resolve any such issue. This Local Union and our licensee have addressed this concern long ago by bargaining alternative language for dispute resolution; other facilities with the same labor management relationship can explore alternative avenues if they choose. It appears changing the law is an easier method for industry to pursue than "owning up" to a prior bad access decision affirmed in circuit courts, which has happened several times in past history. The petition should be dismissed.

Of several access disputes I've overseen in my Local Union, one in particular I offer to your attention is a case answered in 2005. This case captures the atmosphere and spirit of an unescorted access dispute shortly after industry complied with 2003 NRC Security Order EA-02-261 required after the events of September 2001. In FMCS 040707-56079-3, Robert B. Moberly made these key points in his decision that over turned the Company's denial of access decision to an employee who had his unescorted access unilaterally removed in May 2004.

> *"I also credit and give weight to (1) the statements of five supervisors who strongly attest to the Grievant's integrity, character, and security trustworthiness; (2) Grievant's excellent work history of sixteen years with the Company; (3) Grievant's ability to obtain, unescorted access at a another nuclear plant even after he disclosed his prior arrest; (4) Grievant's previous security clearance with the United States Navy to work on a nuclear submarine; and (5) Grievant's forthright demeanor and credibility on the witness stand. Regrettably, it appears from the record that the access control officials and the MRP did not consider the supervisory testimonials or Grievant's work history when it evaluated Grievant's case. I also find the MRP fact-finding process to be less than ideal. The MRP only hears from the access control official whose decision is being appealed. The employee is not given an opportunity to personally appear to present his case. Without full consideration of evidence favoring Grievant's position, the MRP is not given the opportunity to evaluate the totality of the evidence."* (Emphasis Added)

The industry is comprised of a highly skilled and trusted workforce which has given the ultimate gift of record unit reliability and public safety, with safety being our critical mission to accomplish each and every day. Allowing this change as submitted will stifle voices accustomed to demanding improvement. People make mistakes, and even honest and trusted people make mistakes, we are just human, removing the ability to have a fair and just process for dispute of a questionable access decision clashes with the very fabric of being an American working in the private nuclear industry. Enactment of the amendments will deprive potential whistleblowers of protection and, thereby, discourage employees from reporting problems to management or to the NRC.

Our industry contains a culture pursuing continued performance and safety improvement and should remain that way. Clearly in 2004, both the NRC and NEI thought this industry was on the right track for security enhancements which are attached as reminders. It is my opinion we stay on the right track and dismiss this petition. Should you need any further information, please feel free to contact me at your convenience.

Yours truly,

_____

Charlie Nelson
Business Representative

Fact Sheet

United States Nuclear Regulatory Commission
Office of Public Affairs
Washington DC 20555
Telephone: 301/415-8200 E-mail: opa@nrc.gov

Nuclear Security Enhancements Since Sept. 11, 2001

Nuclear Facility Security

The NRC took security seriously well before the September 11, 2001, terrorist attacks and has redoubled its efforts since then in light of the increased threat. Nuclear facilities, including nuclear power plants, already had a number of security and safeguards measures in place in accordance with Commission regulations, making them among the most robust and well-protected civilian facilities in the country. Nevertheless, the events of September 11, 2001, have resulted in enhancements to ensure that these facilities remain secure.

Following the September 2001 terrorist attacks, the NRC immediately advised nuclear facilities to go to the highest level of security in accordance with the system in place at the time. A series of Advisories, Orders, and Regulatory Issue Summaries have been issued to further strengthen security at NRC-licensed facilities including power reactors, decommissioning reactors, independent spent fuel storage installations, research and test reactors, uranium conversion facilities, gaseous diffusion plants, fuel fabrication facilities, certain users of radioactive materials, and transporters of spent fuel and radioactive materials.

Details of the specific actions taken are sensitive, but for facilities such as power reactors, they generally include:

- increased patrols;
- augmented security forces and capabilities;
- additional security posts;
- installation of additional physical barriers;
- vehicle checks at greater stand-off distances;
- enhanced coordination with law enforcement and military authorities;
- more restrictive site access controls for all personnel; and
- expanded, expedited, and more thorough employee background checks.

Security Exercises

The NRC temporarily suspended force-on-force security exercises immediately following the terrorist attacks of September 2001 due to concerns about their impact on security at the plants in the heightened threat environment. In the summer of 2002, tabletop exercises -- facilitated discussions using credible scenarios -- were conducted involving a wide array of Federal, State, and local law enforcement and emergency planning officials.

In February 2003, the NRC resumed security exercises at operating nuclear power plants as part of a pilot project to evaluate the impacts of threat characteristics and security enhancements, as well as to enhance the exercise process. The NRC is currently conducting these exercises at a rate of approximately two per month. Once the pilot program is complete, these exercises will be carried out at each nuclear power plant on a three-year cycle instead of the eight-year cycle that had been implemented prior to September 11, 2001. Additional information is available at: http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/force-on-force.html..

The force-on-force exercise is the primary means of conducting performance-based assessments of a licensee's security force and its ability to protect against the design basis threat as required by NRC regulations. Licensees' security enhancements have reflected the NRC's "defense-in-depth" safety philosophy, in which requirements for plant safety features and mitigation strategies, security measures, and emergency preparedness are addressed in an integrated manner.

Recent force-on-force exercises have utilized Multiple Integrated Laser Engagement System (MILES) equipment to enhance the realism of exercises. MILES gear is a ground combat training system used by the Department of Defense (DOD), the Department of Energy (DOE), and other agencies, using modified weapons fitted with laser transmitters that add realism to exercises by simulating combat between protective and adversary forces.

Security Personnel

The NRC issued Orders on April 29, 2003, to power reactor licensees to augment additional training and qualifications requirements for security personnel. These Orders include more frequent firing of weapons, more realistic training under a broader range of conditions, and firing against moving as well as fixed targets. In order to minimize security personnel fatigue, the agency also issued Orders on the same day to require additional measures for security personnel fitness for duty and work hours controls. It ensures that excessive work hours do not challenge the ability of nuclear power plant security personnel to remain vigilant and effectively perform their duties.

Comprehensive Security Evaluation and Vulnerability Studies

Shortly after September 11, 2001, the NRC undertook a comprehensive re-evaluation of the agency's safeguards and security program, regulations, and procedures that has resulted in

numerous security improvements, most of which are underway. As part of this review, NRC has revised the adversary attributes in the design basis threats (DBTs) for radiological sabotage and for theft or diversion.

The DBT describes the adversary force composition and characteristics against which licensees design their physical protection systems and response strategies. The DBT applies to power reactors and certain nuclear fuel fabrication facilities. Meetings to discuss the proposed revisions have been held with representatives of the nuclear industry cleared to receive such information, and authorized Federal and State agencies. The NRC issued Orders to applicable NRC licensees on April 29, 2003, requiring them to revise their physical security plans and safeguards contingency plans by April 2004, and to have all protective measures in place to meet the revised DBT by October 2004. The NRC has received all licensees' revised security plans..

The NRC believes that most effective strategy for preventing an aircraft attack and protecting our nation's infrastructure continues to be through enhanced measures such as airport passenger and baggage screening, strengthening of cockpit doors and the Air Marshal program.

The NRC has conducted an extensive analysis of the potential vulnerability of nuclear power plants to aircraft attacks. While this analysis is classified, our vulnerability studies confirm that the likelihood of damaging the reactor core and releasing radioactivity that could affect public health and safety is low. Further, the studies confirm that even in the unlikely event of a radiological release due to terrorist use of a large aircraft, NRC's emergency planning basis remains valid. Thus, we believe that nuclear power plant safety, security, and emergency planning programs continue to provide reasonable assurance of adequate protection of the public health and safety.

We recognize that a large aircraft would cause significant damage to a civilian industrial facility and a corresponding psychological impact on the surrounding community and the nation as a whole. Nonetheless, we believe that nuclear power plants remain the most heavily protected civilian facilities in the country. They were so before the events of 9-11 and have been further enhanced since then, by Orders issued by the NRC. In emergency scenarios involving operating reactors, spent fuel pools and dry-cask storage installations, the NRC remains certain that enough time will be available to protect the public near those facilities. Given these enhancements made to safety, security, and emergency preparedness, the potential radiological consequences of an aircraft attack are very low.

In addition, certain interim compensatory measures have been put in place -- improved capabilities to respond to an event that results in damage to large areas of a nuclear power plant from explosions or fires. Additional measures have been put in place to protect against land attacks, including the use of a vehicle bomb, and against water-borne attacks.

The NRC also has taken steps to enhance cybersecurity at nuclear power plants. Since September 11, 2001, the NRC has issued a series of safeguards advisories and orders requiring

nuclear power plant licensees to take certain actions, and many of them address cyber security. Additional measures to enhance cybersecurity are being considered as part of the comprehensive review of NRC's security program.

The NRC is working with appropriate Federal agencies to deal with a potential airborne threat. For example, the NRC has worked with the Federal Aviation Administration and the Transportation Security Administration to put in place a Notice to Airmen advising pilots to not circle or loiter above nuclear power plants or they can expect to be interviewed by law enforcement personnel.

Security Against Dirty Bombs

A radiological dispersal device (RDD) or "dirty bomb" is a conventional explosive containing radioactive material that could be used to spread radioactive contamination. Although these devices would be unlikely to cause serious health effects beyond those caused by the detonation of the explosive, they could have a significant psychological impact, by causing fear, panic, and disruption. Additional information on dirty bombs is available at: http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/dirty-bombs.html .

The NRC has been working with the Department of Energy (DOE), the Federal Bureau of Investigation, the International Atomic Energy Agency and others to enhance physical protection and control of sources of radioactive material that present the highest risk if used by a terrorist in an RDD. The work with DOE is complete and has now been captured in an appendix to the International Atomic Energy Agency's Revised Code of Conduct on the Safety and Security of Radioactive Sources. Elements of "cradle-to-grave" security enhancements will include:

- verification of the legitimacy of applicants for licenses to use radioactive material;
- requirements governing the shipment, storage and use of high-risk sources;
- controls on access to radioactive sources to prevent diversion by an insider;
- tracking and inventorying high-risk sources to ensure they haven't been lost or stolen;
- export and import controls on high-risk sources; and
- more frequent inspections to verify the adequacy of regulatory controls and measures to ensure safe disposal.

In June 2003, the NRC also formed a Materials Security Working Group and a related Steering Committee to work with the States to enhance security for high-risk sources. On June 6, 2003, an Order was issued to all panoramic irradiator and underwater irradiator licensees requiring implementation of additional measures to enhance security. This was the first of a series of additional security actions to be taken for NRC and Agreement State licensees possessing high-risk radioactive material. On Jan. 12, 2004, the NRC issued an Order to manufacturers and distributors of nuclear materials, also requiring implementation of additional security measures. NRC also proposed a rule to enhance security of small gauges that contain radioactive material.

Coordination and Communications

The NRC has expanded its involvement with the Federal Bureau of Investigation, other Federal intelligence and law enforcement agencies, NRC licensees, and military, State and local authorities. Communications have been expanded with the Department of Homeland Security (DHS), the Department of Defense, the Federal Aviation Administration, and others. The NRC also maintains close communications with nuclear regulators in Canada and Mexico, and has discussed security enhancements with nuclear regulatory bodies in other countries (including United Kingdom, France, Germany, Japan, and Romania).

In February 2003, NRC established a protected server system to facilitate exchange of sensitive information between NRC and licensees and authorized State officials. In June 2003, NRC and DHS co-sponsored a two-day Homeland Security Workshop on civilian nuclear security and incident response issues for State officials at NRC headquarters. This workshop was attended by approximately 300 participants from DHS, State Homeland Security Advisors, State Liaison Officers, State Radiation Control Directors, and other Federal and State governments and organizations. This workshop further strengthened NRC and DHS relations with these key State officials by increasing their awareness of DHS and NRC initiatives relating to homeland security and incident response.

NRC Emergency Operations Center and Emergency Plans

The NRC has increased staffing of its Emergency Operations Center in headquarters around the clock that aids in the prompt dissemination of pertinent information to all concerned, including licensees, Federal, and State officials.

The NRC has increased its participation in emergency exercises related to security and counter-terrorism. These exercises have included dealing with dirty bombs, hijacked aircraft, stolen radioactive material, and sabotage of nuclear facilities. In May 2003, the NRC participated in the TOPOFF 2 exercise, the second Congressionally mandated national exercise involving weapons of mass destruction and bioterrorism, and has been extensively involved in the lessons-learned process, particularly in the areas of radiological dispersal device consequence modeling and recovery.

The Agency continues to work with DHS and other Federal agencies on the integration of Federal Response Plans into a unified National Response Plan and National Incident Management System and on refinement of the National Preparedness Policy.

Other Security Actions

To consolidate and streamline selected security, safeguards, and incident response responsibilities and resources, the NRC established an Office of Nuclear Security and Incident Response (NSIR) in April 2002. The creation of NSIR streamlines decision-making, improves

the timeliness of information dissemination, and provides a more visible and effective point of contact and counterpart to the Department of Homeland Security, as well as other Federal agencies. In June 2003, the Agency established the position of Deputy Executive Director for Homeland Protection and Preparedness to increase the agency's attention to cross-cutting issues that affect security, incident response, emergency preparedness, vulnerability assessments and mitigation strategies, and external integration of comprehensive strategies for these areas.

The NRC developed a new Threat Advisory and Protective Measures System that corresponds to the color-coded Homeland Security Advisory System which allows government officials to communicate the nature and degree of terrorist threats consistently nationwide. NRC's system identifies specific actions to be considered by NRC licensees for each threat level to counter projected terrorist threats. If a credible threat emerges against a specific nuclear facility, additional protective measures may be mandated even without a change in the overall threat level.

Security at NRC

A host of enhanced security measures have been put in place at NRC headquarters in Rockville, MD, including the installation of concrete vehicle barriers, increased armed guards, stringent access procedures and ongoing intra-agency communications to keep all NRC employees informed of the latest developments. Security was also bolstered at NRC's four regional offices in King of Prussia, PA, Atlanta, GA, Lisle, IL, and Arlington, TX.

The NRC conducted a comprehensive review and revision of its web site to remove sensitive information which could be of interest to terrorist planners, while it continues to provide the public with appropriate material on the NRC, its role, and other useful information. The NRC also developed and implemented guidelines to identify sensitive information and is developing a new procedure regarding public meetings on security issues.

June 2004

NEWS RELEASE

04-40

Contact NEI's media relations staff at 202/739-8000 during business hours or 703/644-8805 after hours and weekends.

All Nuclear Power Plants Meet NRC Deadline for Security Enhancements

WASHINGTON, D.C., Oct. 28, 2004—All of the 103 commercial nuclear power plants operating at 64 sites in 31 states have met the Nuclear Regulatory Commission's Oct. 29 deadline for implementing more stringent security measures. The NRC in April 2003 issued three security orders that included a requirement that the industry take measures to meet the agency's new description of the size and attributes of an attacking force against which the industry must be able to defend its facilities.

The deadline for implementation of these measures – the culmination of a series of five NRC security orders issued since February 2002 – is Friday.

To meet the NRC's security requirements, the nuclear power plants that provide electricity to one of every five U.S. homes and businesses have taken the following measures:

- increased the size of their paramilitary security forces by 60 percent to a total of 8,000 officers;
- made substantial physical improvements to provide additional protection against vehicle bombs and other potential terrorist assaults;
- increased training for security officers;
- established a rigorous "force on force" mock adversary exercise regime;
- increased security patrols;
- added more security posts;
- increased vehicle standoff distances;
- tightened access controls; and
- enhanced coordination with state and local law enforcement.

NEI
NUCLEAR ENERGY INSTITUTE

SUITE 400
1776 I STREET, NW
WASHINGTON, DC
20006–3708
202.739.8000
www.nei.org

- more -

"These security enhancements will continue to make nuclear power plants the most secure industrial facilities in America," said Marvin Fertel, the Nuclear Energy Institute's chief nuclear officer.

Expenditures for the security manpower and capital improvements total in excess of $1 billion since 2001. This sum is above and beyond the hundreds of millions of dollars that cumulatively had been spent on security prior to the Sept. 11 terrorist attacks.

"The nuclear energy industry is fully committed to protecting its employees, the public and its assets," Fertel said. "Through voluntary actions and in response to regulatory requirements, we have taken extraordinary measures to beef up physical and cyber security, improve training, expand our paramilitary security forces and coordinate extensively with government entities on security matters."

With federal oversight from the NRC, the industry systematically reviews and challenges its security programs to further strengthen its robust defenses. Fertel cautioned, however, that on the heels of the latest security enhancements, there must be a period of regulatory stability so industry can fully integrate the new security programs into plant operations.

While this integration is taking place, Congress and other policymakers should consider whether homeland security resources are being used properly across the nation's critical infrastructure, Fertel said. Industries that are not regulated by an entity with the responsibility and authority similar to that of the NRC were not as secure as nuclear power plants prior to 2001, and have not kept pace with the security enhancements made at nuclear plants during the past three years.

With these recent enhancements to on-site security, the industry believes the focus should shift to enhancing the integrated responses of all off-site entities in support of plants' security forces. Consideration of integrated off-site security responses and emergency preparedness activities at commercial nuclear facilities has intensified recently with the formation of a Nuclear Sector Coordinating Council. The council consists of industry leaders and is partnered with the federal government's Nuclear Sector Government Coordinating Council, which is led by Department of Homeland Security, NRC and Department of Energy representatives.

The coordinating council was formed in response to a presidential homeland security directive, and it held its first official meeting on Oct. 13 in Washington, D.C. Council-level strategy meetings will be held at least quarterly. The mission of the coordinating council is to identify and implement ways to enhance security and emergency preparedness around nuclear facilities, primarily beyond the exclusive responsibility of a nuclear plant's security force.

###

The Nuclear Energy Institute is the nuclear energy industry's policy organization. This news release and additional information about nuclear energy are available on NEI's Internet site at http://www.nei.org.

NEWS RELEASE

04-35

Contact NEI's media relations staff at 202/739-8000 during business hours or 703/644-8805 after hours and weekends.

Nuclear Power Plants Are Most Secure Industrial Facilities in U.S., NEI Tells Congress

WASHINGTON, D.C., Sept. 14, 2004—The nuclear energy industry expects to meet new federal security requirements—further strengthening the robust defenses at vital nuclear power plants—by the government's Oct. 29 deadline, an industry leader told a congressional panel today.

NEI
NUCLEAR ENERGY INSTITUTE

SUITE 400
1776 I STREET, NW
WASHINGTON, DC
20006–3708
202.739.8000
www.nei.org

"Each nuclear power plant is on schedule to meet the requirements of the most recent Nuclear Regulatory Commission security orders by the October 29 deadline," Marvin Fertel, the Nuclear Energy Institute's chief nuclear officer, told the House Committee on Government Reform's National Security, Emerging Threats and International Relations Subcommittee.

The security enhancements will continue to make nuclear power plants "a model for industrial security in America" and solidify their position as the nation's best-defended industrial facilities, Fertel said.

"Our defenses were exceptional prior to the September 11, 2001, terrorist attacks, and they are even 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," he said.

With oversight from the Nuclear Regulatory Commission (NRC), the industry constantly reviews and re-evaluates its security programs to further strengthen its robust defenses, Fertel said.

He cautioned, however, that on the heels of the latest security enhancements, there should be a period of "regulatory stability" so the industry can integrate the new security programs fully into plant operations.

"The NRC has recognized that the commercial nuclear energy industry has reached the maximum level of security enhancements that can be expected from a private entity. Further increases to nuclear plant security requirements could have serious policy implications," he said.

-more-

Fertel detailed for members of Congress the many steps that the industry has taken over the past three years to strengthen security, including the recent formation of the Nuclear Sector Coordinating Committee with the U.S. Department of Homeland Security.

"The committee provides a forum for integrating on-site and off-site resources for threats that exceed our stand-alone capabilities. The industry is fully committed to working with all levels of government in providing the best security possible to deter an attack and to provide the best possible response should one occur," he said.

By the end of this year, in meeting security requirements imposed by the NRC after the terrorist attacks, the nuclear energy industry will have spent an additional $1 billion, Fertel said.

"As a result of these new requirements, the number of security officers at our 64 plant sites has increased from approximately 5,000 to 8,000, an average of 125 officers per site. Other changes at nuclear plants 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.

"The physical improvements and equipment upgrades comprise the majority of this $1 billion total, yet the industry also has spent hundreds of millions of dollars on additional personnel."

Congress and other policymakers should consider whether homeland security resources are being used properly, Fertel said, because industries that are not regulated by an entity with authority similar to that which the NRC possesses were not as secure as nuclear power plants prior to Sept. 11, 2001, and have not kept pace with the security enhancements made at nuclear plants since the attacks occurred.

"A comprehensive homeland security policy identifies targets based upon risk and allocates resources appropriately," he said. "Risk assessments by notable security authorities have found – based on past terrorist targets – that nuclear plants are hardened targets and are considerably less likely to be the focus of terrorist attacks."

One hundred and three reactors operating in 31 states provide electricity to one of every five U.S. homes and businesses.

###

The Nuclear Energy Institute is the nuclear energy industry's policy organization. This news release and additional information about nuclear energy are available on NEI's Internet site at http://www.nei.org.