U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Backgrounder

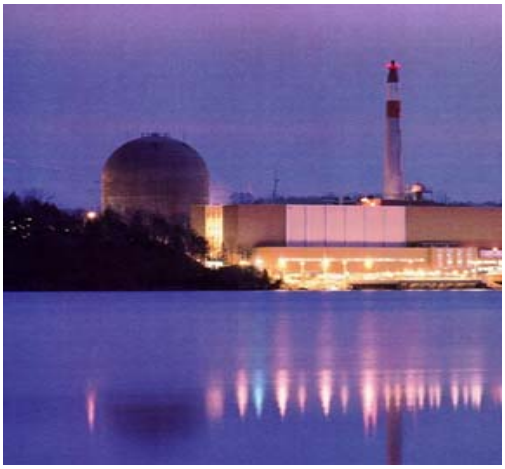
Office of Public Affairs
Telephone: 301/415-8200 E-mail: opa@nrc.gov

Nuclear Security

Background

While security of the nuclear facilities and materials the NRC regulates has always been a priority, the terrorist attack of Sept. 11, 2001, brought heightened scrutiny and spurred more stringent security requirements. Today, NRC-regulated nuclear facilities are among the most secure of the nation's critical infrastructure. In fact, one member of Congress rated nuclear plant security the strongest among the nation's civilian infrastructure.

This heightened security is achieved in layers, with multiple approaches concurrently at work – just as safety in nuclear power plants is accomplished through duplicate back-up systems. To begin with, nuclear power plants are inherently secure, robust structures, built to withstand hurricanes, tornadoes and earthquakes. Additional security measures are in place: well trained and armed security officers; equipment and structures, including physical barriers, intrusion detection and surveillance systems; and access controls. Another layer of protection is in place for coordinating threat information and response. The NRC works closely with the Department of Homeland Security (DHS), FBI, intelligence agencies, the departments of Defense and Energy, states, and local law enforcement. These relationships ensure the NRC can act quickly on any threats that might affect its licensed facilities and allows effective emergency response from "outside the fence" should a serious terrorist attack occur.



While many of the details of the NRC's security requirements are withheld to avoid assisting potential adversaries, general information about the security enhancements of the past few years is available to the general public from a variety of sources, including NRC's Web site, NRC publications, and other publicly available sources.

Nuclear Facility Security

For several years following 9/11, the NRC required many security enhancements at its licensed power reactors, decommissioning reactors, independent spent fuel storage installations, research and test reactors, uranium conversion facilities, gaseous diffusion plants, fuel fabrication facilities, large irradiators, manufacturers and distributors, transportation, and licensees with greater than IAEA category 2 material. The NRC directed nuclear power plants and fuel

fabrication facilities to upgrade their physical security plans, security officer training and qualification plans, and contingency plans. These facilities now have, among other heightened measures:

- More patrols
- Stronger and more capable security forces
- Additional physical barriers
- Greater stand-off distances for vehicle checks
- More restrictive site access controls
- Enhanced emergency preparedness and response plans

Nuclear power plants and category I fuel fabrication facilities must show they can defend against a set of adversary characteristics outlined in the NRC's Design Basis Threat (DBT). While the details of the DBT are not public, in general, it outlines threats and adversary characteristics that these facilities must protect against with high assurance. The NRC supplemented the DBT in April 2003 and March 2006 to incorporate insights from the 9/11 attacks. In January 2007, the NRC amended 10 CFR 73.1 and issued a final rule consolidating the supplemental requirements established by the April 29, 2003 and March 20, 2006, DBTs orders with the existing DBT requirements in NRC regulations. The final rule also met the NRC's obligation under the 2005 Energy Policy Act to initiate and complete a rulemaking revising the DBT, considering the 12 factors specified in the law. The NRC is constantly re-evaluating the threat environment and will consider additional changes to the DBT in the future, if warranted.

Security Inspections and Rulemaking

The NRC has also significantly increased its oversight of security capabilities. In 2000, NRC inspectors spent about 40 staff-weeks a year at nuclear power plants directly inspecting security (excluding special "force-on-force inspections"). By 2003, this inspection effort had increased five-fold to 205 staff-weeks. These inspections specifically focused on the implementation of "compensatory measures" the NRC required after the 2001 attacks to address the new threat environment. In 2004, the NRC implemented a new "baseline inspection program" for security and by 2005, direct staff inspections at nuclear power plants had increased further to about 400 staff-weeks a year.

The NRC is also proposing rules for all facilities to amend current security regulations and add new security requirements. The proposed rulemaking for power reactors would: 1) apply system-wide security requirements imposed by Commission Orders issued after the terrorist attacks of Sept. 11, 2001, based upon experience and insights gained by the Commission during implementation; 2) fulfill certain provisions of the Energy Policy Act of 2005; 3) add several new requirements that resulted from insights from implementation of the security orders, review of site security plans, and implementation of the enhanced baseline inspection program and force-on-force inspections; 4) ensure enhanced security is integral to new reactors; and 5) impose requirements to assess and manage site activities that can adversely affect safety and security. It is anticipated that this rule will go into effect during calendar year 2009.

Force-on-Force Performance Evaluations

The NRC sets the rules and then tests the security response at nuclear power and category I fuel cycle facilities with security performance evaluations called "force-on-force" inspections. In these inspections, a specially trained mock adversary force "attacks" the facility. In 2004, the NRC implemented more realistic force-on-force exercises on a more aggressive schedule that

tests facilities more frequently (at least every three years) and under more challenging expectations. In December 2007, the NRC completed the first three-year cycle of current force-on-force inspection program and reported the results to Congress in June 2008. The second three-year cycle began in January 2008. Efforts are ongoing to further enhance realism and addresses "lessons learned" from these exercises.

Security Personnel

One of the most important components of security programs at nuclear power facilities is the security force. Over the past five years, the NRC has required power plants to add more training and higher qualification standards for security personnel, while substantially increasing the number of officers on the force. Plant security officers, for example, must now be trained under more realistic conditions and against moving targets. In order to minimize security personnel fatigue and ensure a vigilant and effective security force, the NRC has instituted additional fitness-for-duty requirements and work hours controls.

In accordance with the Energy Policy Act of 2005, the NRC has also strengthened requirements for fingerprinting and background checks for various types of licensees and certificate holders. On Jan. 4, 2006, the NRC entered into an agreement with the federal government's Terrorist Screening Center to review records of individuals with unescorted access to nuclear power reactor facilities. This collaborative effort automated and streamlined the collection and dissemination of information used to determine the trustworthiness of individuals who have unescorted access to certain vital areas of nuclear power plants. It also enhances the process of identifying anyone with access to these areas who may pose a threat to national security.

Research

Research has always played a large part in supporting the NRC's safety mission. Since 9/11, changes in the threat environment and improvements in technology that allow more sophisticated analyses, have accelerated the pace of power plant research and security studies. For example, the NRC initiated a security and engineering review based on the September 11th events. The review looked at what might happen if terrorists used an aircraft to attack a nuclear power plant. The NRC also assessed the potential consequences of other types of terrorist attacks. National experts from Department of Energy (DOE) laboratories used state-of-the-art experiments and structural and fire analyses to assist the NRC. While the details are classified, the studies confirm that the plants are robust, and the likelihood of a radioactive release affecting public health and safety is low. Another study analyzed the ability of nuclear power plants to withstand damage to, or loss of, large areas of the plant caused by a range of postulated attacks that could result in large fires and explosions. After examining a number of emergency scenarios involving operating reactors, spent fuel pools and dry-cask storage installations, the NRC has concluded that the existing planning basis used to develop nuclear power plant emergency plans remains valid and is confident that the public near those facilities can be adequately protected should an attack occur. As part of these analyses, enhancements were identified and the NRC ordered changes at nuclear power plants. Moreover, based on insights from these studies, industry best practices, and lessons-learned from the response to the attacks of Sept. 11, 2001, additional mitigating capabilities have been put in place at all nuclear power plants.

Cyber Security

While the September 11 attacks didn't have a "cyber" component, cyber security is a growing and serious issue. The NRC has already issued a series of advisories and orders requiring nuclear power plants to take certain actions, including enhancing protection of their computer systems. Several new rulemakings are proposing further cyber security requirements. One proposed rule would require nuclear power plants to implement strategies to protect computer systems, detect cyber attacks, and isolate and neutralize cyber intruders. However, it is important to note that computer systems that help operate the reactors and other power reactor safety equipment are isolated from the internet to protect against outside intrusion. As suggested by the Energy Policy Act of 2005, the Commission added a cyber threat component to the DBT in January 2007. In addition, the NRC routinely interacts with the DHS's National Cyber Security Division to coordinate federal cyber security activities in the nuclear sector.

Security Against "Dirty Bombs"

The security of radioactive materials has been a concern of NRC due to the possibility that such material could be used to build a radiological dispersal device – a type of conventional explosive combined with radioactive material that could spread radioactive contamination. While a so called "dirty bomb" is unlikely to cause substantial deaths or even contaminate a very large area, it could cause panic and disruption. The NRC works with its Agreement States, DHS, DOE, the FBI, and the International Atomic Energy Agency, as well as manufacturers and distributors of nuclear materials, to protect certain radioactive material from theft or diversion.

In recent years, required security measures related to nuclear and radioactive material have been increased. Improvements and upgrades have been made to the Nuclear Materials Management and Safeguards System, a joint NRC-DOE database that captures the movement and location of certain forms and quantities of nuclear material. Also, development of the National Source Tracking System is progressing and is slated for operation at the beginning of 2009. This system will allow radioactive sources in quantities of concern to be closely tracked. In the meantime, the NRC's Interim Inventory of Radioactive Sources, established to address international requirements on source tracking, has been updated annually. This inventory has proven to be a valuable resource and has been used several times to ensure the safety and security of radiation sources following hurricanes. Also, these improvements now allow U.S. Customs and Border Protection agents to get near real-time validation of NRC licenses associated with materials coming into the U.S.

To be ready in the event of a radiological or nuclear-related terrorist event, the NRC and other federal agencies have developed guidance for officials to use in response and long-term recovery planning. The NRC joined DHS, the Environmental Protection Agency (EPA), the Department of Defense, DOE and other federal Agencies to develop the guidance. This guidance establishes recommendations for local, state, tribal, territorial and federal responders and decision makers in planning for a Radiological Dispersal Device (RDD) or an Improvised Nuclear Device (IND) attack. The guides are flexible and use an optimization process to address the broad range of scenarios that could occur – a range larger than that addressed by most previous programs. DHS published the "Planning Guidance for Protection and Recovery Following Radiological Dispersal Device and Improvised Nuclear Device Incidents," in the *Federal Register* on August 1, 2008 [73 FR 45029].

Coordination and Communications

The NRC coordinates with many federal organizations in assuring adequate protection of its licensees. One tangible example is the National Infrastructure Protection Plan, which, when coupled with the Nuclear Sector Specific Plan and National Response Framework, facilitates the sharing of information and provides for a coordinated, comprehensive response to threats and events. Federally integrated response is also illustrated by DHS's decision to conduct infrastructure reviews in the nuclear sector, making it a model for future reviews of security at other critical infrastructure. The Comprehensive Review initiative (a DHS-led program to evaluate national critical infrastructure protection capabilities) which was completed in 2007, integrated a full range of security, law enforcement and emergency preparedness professionals to identify strengths and potential weaknesses of the nation's critical infrastructure and key resources. Nuclear power plants were identified as the initial area for review because of the high level of planning already in place. Efforts are now in place to address certain issues that were identified during the Comprehensive Reviews.

The NRC has also developed a Threat Advisory and Protective Measures System that corresponds to the color-coded Homeland Security Advisory System. The NRC 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.

The timely sharing of accurate information among the NRC, other federal agencies and the nuclear industry is critical to preventing or mitigating the effects of terrorist attacks. NRC staff members are assigned to the Domestic Nuclear Detection Office, the National Counterterrorism Center and the DHS Infrastructure Protection Office to enhance inter-organizational communication and support the integrated assessment of security related information. The NRC has also entered into agreements with the Federal Aviation Administration and the North American Aerospace Defense Command to provide early warning of airborne threats to NRC-licensed facilities. Additionally, the NRC Operations Center, located in the agency's headquarters in Rockville, Md., provides an around-the-clock conduit for disseminating information and coordinating response, and NRC's highly-trained specialists review intelligence and threat-related information from a range of sources in order to assess suspicious activity related to its licensees. Secure communications systems also allow the NRC to communicate with nuclear regulators in other countries.

The NRC has always been committed to open communication with the public. However, since Sept. 11th, the NRC realized that security-related information it routinely made public could possibly aid potential adversaries seeking to steal or divert radioactive materials or attack or sabotage a nuclear power plant. With that reality, NRC revised its information dissemination policy, and the public is provided only limited information on regulatory decisions or actions involving security inspection, assessment or enforcement. The Commission regularly reassesses this policy and in mid-2006 began making certain results of its security inspection program for nuclear power plants available to the public. The NRC has also conducted a number of public

meetings on security and emergency preparedness, allowing the flow of some information to external stakeholders and the public without jeopardizing national security. The NRC is continuing to look at achieving a proper balance between openness and security of its information, and additional changes may be forthcoming in 2009.

NRC Emergency Operations Center and Emergency Plans

The NRC's Emergency Operations Center is staffed around the clock to receive information regarding licensed nuclear materials related events, assist in emergency response activities, and promptly notify other Federal Agencies of those events. In recent years, ongoing upgrades to the center have enhanced effectiveness of response and coordination. Similar upgrades have also been completed in the NRC's four Regional Incident Response Centers. The NRC has increased its participation in emergency exercises related to security and counter-terrorism. Recent exercises have included such scenarios as dirty bombs, hijacked aircraft, stolen radioactive material, and sabotage of nuclear facilities. The NRC also participates in national-level interagency exercises.

In response to the current heightened security environment, the nuclear industry through the Nuclear Energy Institute (NEI), with NRC support, has taken the initiative to develop guidelines addressing the unique challenges of security events to existing EP programs. The objective of this guidance is to continue to ensure public health and safety in the event of a security-based event at a U.S. nuclear power plant.

The NEI guidelines detail a phased approach for the incorporation of hostile action based scenarios into the routine EP drill and exercise program in response to Attachment 6 of NRC Bulletin 2005-02, "Emergency Preparedness and Response Actions for Security-Based Events." Specifically, the guidelines outline the conduct of a hostile action based scenario as an "off-year" EP drill by each power plant over a 3-year period ending in 2010. These hostile action based EP drills, commonly known as "Phase 3 Drills," are not currently evaluated by either the NRC or FEMA, and therefore, provide a "no fault" opportunity for licensees to demonstrate responses to the unique challenges security-based events pose to existing EP programs. Lessons learned from these drills are intended to support formal implementation of hostile action based scenarios into each licensee's exercise cycle in the near future.

In addition to routinely participating in emergency exercises, the NRC emergency response organization also responds to actual events involving NRC licensees. Following both exercises and actual event response, the NRC critiques its actions and continually improves its response capabilities. The NRC participated in the federal review of lessons learned from Hurricane Katrina, and implemented changes in procedure and protocol to enhance readiness for future hurricane seasons.

The NRC believes that good planning leads to good response in all types of events, including security-related situations. In addition to mandatory directives and advisories issued after the 2001 attacks, the NRC required nuclear power plants to implement security-related enhancements to their emergency preparedness (EP) programs in 2005. These changes incorporated lessons learned from licensee inspections, observations of EP drills and exercises, and comments received from a variety of stakeholders, including state and local emergency response agencies and the public. Additionally, the NRC is pursuing a series of enhancements to the existing EP regulations and guidance. The staff solicited and received a large number of

comments from stakeholders and considered those comments in the development of the proposed regulation and guidance updates. The NRC will continue to interact with appropriate stakeholders to improve EP capabilities at nuclear power plants and nuclear materials facilities.

October 2008