U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Protecting Our Nation

A Report of the U.S. Nuclear Regulatory Commission

Office of Nuclear Security and Incident Response

Acknowledgements

Paul J. Kelley, Jr.

Rollie D. Berry, III

Rebecca A. Clinton

Holly A. Phillips

Eric J. Stahl

Amy J. Steen

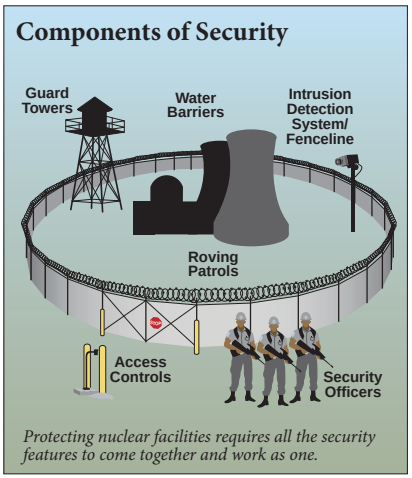
Table of Contents

Executive Summary

For over 30 years, the U.S. Nuclear Regulatory Commission (NRC) has maintained effective nuclear security, emergency preparedness, and incident response programs. The NRC requires safe and secure operations at nuclear facilities. Safety refers to operating the facility in a manner that protects the public and the environment. Security refers to protecting the facility from adversaries who wish to harm people and the environment. Safety and security are accomplished by using people, equipment, and physical protection.

Chairman Gregory B. Jaczko speaks at The Heritage Foundation in Washington, D.C.

Security is achieved in layers, with multiple approaches at work. For example, nuclear power plants are inherently secure, robust structures that are designed and built to withstand hurricanes, tornadoes, and earthquakes. In addition, well-trained, armed security guards, physical barriers, access controls, and intrusion detection and surveillance systems protect certain NRC-licensed facilities, such as commercial power reactors. For other applicable NRC-and Agreement State-licensed facilities, the NRC has required implementation of enhanced security requirements.



Protecting nuclear facilities requires all the security features to come together and work as one.

Another layer of protection is in place for coordinating threat information and response. The NRC works closely with Federal, State, and local authorities. These relationships ensure that the NRC can act quickly to disseminate threat information to licensees and allow effective emergency response in the event of an attack. Together, these layers of defense provide a level

of security likely second to none in the national commercial sector.

Among the topics covered in this document, the following highlight major NRC initiatives in nuclear security:

NRC Executive Director for Operations, R. William Borchardt with two of his deputies, Darren B. Ash (left) and Bruce S. Mallet (right).

- Increased the level of realism in force-on-force mock attack exercises while ensuring the safety of plant employees and the public. The program continually applies lessons learned from previous years.
- Amended security regulations for nuclear power plants and will continue to verify that licensees have implemented the amended regulations through licensing reviews, inspections and force-on-force exercises.
- Substantially increased oversight of security activities at all nuclear power plants through the security baseline inspection program.
- Revised its security regulations to include cyber-security requirements.
- Continued efforts to safely and securely transport shipments of spent fuel along NRC-approved routes using NRC-approved packages.
- Implemented the National Source Tracking System database, which enhances accountability for certain radioactive materials and requires licensees to report the manufacture, transfer, receipt, disassembly, and disposal of nationally tracked radioactive sources.
- Coordinated activities related to the nuclear industry's efforts to conduct emergency preparedness exercises initiated by hostile actions and preparing the industry and offsite response organizations for implementing hostile action-based exercises proposed by new rulemaking.
- Added staff, improved emergency response procedures, and upgraded equipment in the NRC Headquarters Operations Center.

Introduction

The U.S. Nuclear Regulatory Commission (NRC) is committed to protecting the health and safety of the public, promoting the common defense and security, and protecting the environment. The terrorist attacks on September 11, 2001, reaffirmed the need for collective vigilance, enhanced security, and improved emergency preparedness and incident response capabilities across the Nation's critical infrastructure. As a result, the NRC conducted thorough evaluations of the agency's security programs and enhanced security at NRC-regulated facilities.

Commissioner Kristine L. Svinicki speaks at the Regulatory Information Conference.

The events of September 11, 2001, also highlighted the need to reexamine the organization of the NRC itself. As a result, the NRC created the Office of Nuclear Security and Incident

Response (NSIR) in April 2002 to more effectively assemble staff expertise. In addition to reassigning staff from other areas within the NRC, NSIR hired experts in security with civilian and military experience. Today, NRC-regulated nuclear facilities are among the most secure in the Nation's critical infrastructure.

This document describes the highlights of a comprehensive sequence of actions that the NRC has taken to strengthen the security of U.S. nuclear facilities and radioactive materials.

Communications

Public meeting on security requirements for transporting certain radioactive material.

Effective communication among the NRC; NRC-licensed facilities and certificate holders; and Federal, State, and local governments is an important part of protecting nuclear facilities from acts of terrorism. Since September 11, 2001, the NRC has continued to enhance its communications. These upgrades include a protected computer server system to provide quick and easy exchange of sensitive security information with licensees and authorized government officials.

The NRC works with a variety of partners to fulfill its mission and maintains close working relationships with State officials and members of Congress. The NRC regularly communicates with Federal partners, including the following, about policy and programs:

- U.S. Department of Defense
- U.S. Department of Energy (DOE)
- DOE-National Nuclear Security Administration
- U.S. Department of Homeland Security (DHS)
- DHS-Federal Emergency Management Agency (FEMA)
- DHS-Transportation Safety Administration
- DHS-Domestic Nuclear Detection Office
- U.S. Department of Transportation
- Federal Aviation Administration
- Federal Bureau of Investigation
- National Security Council
- North American Aerospace Defense Command
- U.S. Northern Command
- National Counterterrorism Center

In addition, the NRC talks directly to other Federal agencies about specific threats. For example, the NRC communicates with the North American Aerospace Defense Command using a telephone alert system to share information about potential aircraft threats against NRC-regulated nuclear facilities. This coordination lays the foundation for ongoing national efforts to detect, prevent, and respond to terrorist attacks.

The NRC has also developed a threat response procedure that corresponds to the color-coded DHS Homeland Security Advisory System. The NRC system identifies specific actions that NRC-licensed facilities should consider taking for each threat level. If a credible threat emerges against a specific nuclear facility, additional protective measures may be mandated.

The NRC has a long history of promoting openness in its regulatory and decisionmaking processes. However, the NRC must prevent unauthorized individuals or those without a need to know from gaining access to sensitive information that might compromise the security at NRC-regulated facilities. As a result, the NRC must balance its commitment to openness with the need to prevent release of sensitive information. The NRC continues to explore areas in which sharing information will result in a better informed and prepared Nation.

Intelligence

The NRC's intelligence staff reviews, analyzes, coordinates, and distributes threat and intelligence information about the U.S. civilian nuclear sector only to individuals with a need to know and who have clearances. The intelligence staff constantly monitors the domestic and overseas threat environments for credible threats to NRC licensees. The NRC staff also serves as a liaison and coordinates with other organizations and Federal agencies. The NRC ensures that its licensees; its Agreement States; and Federal, State, and local authorities promptly receive notification of any threat or security incident. In addition, the staff annually reviews and briefs the Commission on recommended changes to the NRC's design-basis threat (DBT) based on the evolving characteristics of terrorists. The DBT describes the basic adversary force that nuclear power plants and Category I fuel cycle facilities must defend against.

The central mission of the NRC intelligence staff is to evaluate and warn of possible threats against an NRC or Agreement State licensee. Since the 1970s, the NRC has assessed and, in some cases, investigated a variety of threats to licensed nuclear facilities and radioactive materials. These threat assessments could provide indications and warnings of potential attacks or other malevolent activities directed at nuclear facilities. The intelligence staff assesses threats by reviewing thousands of pieces of message traffic, evaluating intelligence products, and routinely communicating with other intelligence and law enforcement agencies.

In the event of an actual threat, the NRC's intelligence staff forms the core of an interdisciplinary

team that assesses the credibility of a communicated threat and recommends protective actions to licensees. The NRC's intelligence staff also has a duty officer who is on call 24 hours a day, 7 days a week to respond to security events and suspicious incidents at NRC-licensed facilities.

To share threat information rapidly, the NRC developed the Threat Advisory System in the mid-1980s. Threat advisories are nonpublic, rapid communications from the NRC to licensees that provide information on changes to the threat environment. If the NRC receives information about a possible threat to one of its licensees, it issues a threat advisory informing the site and advising protective measures. Advisories also include guidance suggesting specific actions that licensees can take to strengthen their capabilities to defend against any threat. The NRC expanded the Threat Advisory System after September 11, 2001, in response to the evolving nature of the threat.

Design-Basis Threat

The DBT describes the basic adversary force against that nuclear power plants and Category I fuel cycle facilities must defend. The DBTs are based on realistic assumptions about the threat capabilities of terrorist groups and organizations. They are developed by working with national experts and are based on classified and other sensitive information. The NRC also relies on the intelligence community, law enforcement agencies, and State and local governments to provide accurate and timely information about the capabilities and activities of these groups.

Changes to the DBT have warranted an increase in physical security, including enhancements to vehicle barriers.

Following the September 11, 2001, terrorist attacks, the NRC conducted a thorough review of the DBTs to ensure that nuclear power plants and other licensed facilities continued to have effective security measures in place that account for the evolving threat environment. The NRC issued orders that upgraded the DBTs as a result of this review. These orders were later incorporated in a revised DBT rule that was issued in 2007. The new rule reflects insights gained by the NRC since September 11, 2001, the latest threat information and a strengthened cyber threat component, as suggested by Congress and the public.

The rule does not require protection against a deliberate hit by a large aircraft. The active protection of the Nation against airborne threats is the responsibility of other federal organizations, including the military. The NRC is an active partner

Onsite security personnel participate in firearms training.

Security barriers provide one of the many layers of physical protection.

with other Federal, State, and local authorities in constant surveillance of the threat environment and will adjust regulatory actions or requirements if necessary. The NRC conducted several comprehensive studies, which determined that an aircraft impact is unlikely to result in core damage or a radiological release. The NRC has also required its licensees to take steps to mitigate the effects of large fires and explosions from any type of initiating event.

The NRC staff regularly reviews the DBT against the current threat intelligence, both domestic and overseas, to determine if any changes to the DBT are warranted. Specific characteristics of the DBT are not publicly available in order to protect sensitive information that could potentially aid an adversary. In general, the changes to the DBT have warranted the need for enhancements at licensed facilities, including the following:

- increased patrols;
- additional security posts and physical barriers;
- vehicle checks from greater standoff distances;
- increased training for security and emergency response personnel;
- improved equipment and communication; and
- increased site access controls for personnel, including more thorough employee background checks.

Security Baseline Inspections

The NRC's security baseline inspection program is the primary way in which the agency ensures that nuclear power plants operate according to security regulations. Under the program, regional experts from NRC offices in the Philadelphia, Atlanta, Chicago, and Dallas areas carry out most security inspections. The experts provide firsthand, independent assessments of plant conditions and performance.

An NRC inspector gathers information at a nuclear power plant.

The NRC has significantly increased its oversight of security at nuclear power plants since September 11, 2001. The NRC issued orders to nuclear power plants to increase their security, and the NRC in turn enhanced its Security Baseline Inspection Program to evaluate and inspect this additional security. These enhanced inspections specifically focus on the implementing measures that the NRC put in place to address the post-September 11, 2001, threat environment.

Inspectors monitor the licensee's security-related activities throughout the year and document their inspection findings in writing for the plant management. They conduct follow-up inspections to ensure that the licensee has made the necessary corrections. Security baseline inspections cover the following four key attributes:

(1) Access Authorization—Individuals must meet certain requirements to gain unescorted access within a nuclear power plant. The licensee is responsible for granting, denying, or revoking unescorted access authorization. These requirements include, but are not limited to, criminal background checks, behavioral observation, and drug and alcohol testing.

(2) Access Control—The licensee must control and limit activities in designated areas of the power plant

facility. Access is limited to those personnel who are authorized to be in these areas.

(3) Physical Protection—People, procedures, and equipment must be integrated to protect against theft, sabotage, or other malevolent attacks. This requirement provides assurance that the physical security system can protect against the DBT.

(4) Contingency Response—Licensees must develop a plan that guides the response of licensee personnel to thefts, threats, and radiological sabotage.

The NRC's overall evaluation of licensee performance takes into consideration the results of security inspections. However, if a significant security issue is found, the NRC requires the licensee to resolve the issue promptly. If necessary, the NRC can take enforcement action that includes civil penalties. Information related to these inspections are available to the public. In 2009, the NRC amended security regulations and added new security requirements for nuclear power plants that need to be in place in 2010. The NRC staff will inspect licensees to ensure that they have properly implemented the new security requirements.

Security Programs at NRC-Licensed Facilities that Ensure Trustworthiness and Reliability

Four main programs have been implemented at each nuclear power plant and Category I fuel cycle facility to ensure that those individuals who gain and maintain access to the facilities are trustworthy and reliable. Each of the four programs is described below in more detail.

Many licensees use biometrics as part of their access requirements.

Access Authorization Program

The NRC requires licensees to control access to nuclear facilities. Before new employees or contractor employees are allowed unescorted access to the protected area of nuclear power plants and Category I fuel cycle facilities, they must pass several evaluations and background checks to determine if they are trustworthy and reliable. These evaluations include drug and alcohol screening, psychological evaluations, a check with former employers, and an assessment of education records, criminal histories (through the Federal Bureau of Investigation), and credit histories.

The NRC recently strengthened many elements of the access authorization program. The access authorization requirements now include the following:

- covers additional individuals who have electronic (cyber) means to adversely impact facility safety, security, or emergency preparedness;
- enhanced psychological assessments;
- increased information sharing between reactor licensees;
- expanded behavioral observation;
- reinvestigations of criminal and credit history records for all individuals with unescorted access; and
- a 5-year psychological reassessment for certain critical job functions.

Fitness-for-Duty Program

Companies that operate nuclear power plants and Category I fuel cycle facilities demand and ensure that personnel perform their duties in a safe, reliable, and trustworthy manner, including not working under the influence of legal or illegal substances or being mentally or physically impaired from other causes that would hinder their abilities to perform their duties. Employees who have unescorted access to the facility's protected area must maintain their fitness for duty. The NRC requires companies to conduct random drug and alcohol testing of their employees. As a result, at least one-half of all employees are tested annually.

The NRC requires nuclear power plant licensees to impose work-hour limits on security force personnel and to develop procedures to evaluate their fatigue. In 2008, the NRC published a rule updating its regulations on work-hour controls. The new requirements limit the work hours of security personnel and safety-sensitive workers, who operate and work on safety equipment, at nuclear power plants. They also identify the process and expectations of self-referrals for fatigue. Licensees are required to conduct a documented fatigue assessment if individuals report that they are unfit for work because of fatigue or if workers are observed to be inattentive. Licensees are also required to relieve individuals of covered duties if they self-report for fatigue.

In addition to enhancing the agency's fatigue management requirements, the NRC has also modified requirements for drug and alcohol testing of security personnel and others who perform safety-sensitive work at nuclear power plants. The NRC requires drug and alcohol testing to detect and deter substance abuse. The modified requirements include additional procedures to ensure the integrity of the testing process and to update testing procedures to reflect advances in drug and alcohol testing technologies.

Behavioral Observation Program

The NRC requires both nuclear power plant and Category I fuel cycle facility licensees to implement a behavioral observation program. This program is conducted by multiple personnel within an NRC-licensed facility who are trained specifically on behavioral observation techniques. The program looks for individual behavioral changes that, if unmonitored or left unaddressed, could

lead to acts which could be detrimental to public safety. Employees are offered counseling if they have job performance problems or exhibit unusual behavior. Similarly, anyone who appears to be under the influence of drugs or alcohol is immediately removed from the work area for evaluation under the licensee's fitness-for-duty program.

Insider Mitigation Program

The insider mitigation program is the integration of the access authorization, fitness-for-duty, and behavioral observation programs at each nuclear power plant and Category I fuel cycle facility. The insider mitigation program helps ensure that those gaining and maintaining unescorted access within an NRC-licensed facility do not pose a potential insider threat. An insider threat is a person who could use the knowledge or access gained by his or her job at a facility to potentially aid an adversary. These programs are essential to the overall security of nuclear power plants and Category I fuel cycle facilities.

Force-on-Force Security Inspections

An adversary force approaches a nuclear power plant during a force-on-force training exercise.

Force-on-force security inspections are one of the most significant components of the NRC's security inspection program. It provides insight into the NRC's efforts to evaluate and improve the effectiveness of the security programs at power plants and Category I fuel cycle facilities. The NRC has carried out inspections, similar in scope and purpose, regularly since 1991. They are an essential part of the oversight of the security of these facilities. Force-on-force inspections assess the ability of these facilities to defend against the DBT.

A full force-on-force inspection spans several weeks. It includes both tabletop drills and simulated combat that takes place between a mock commando-type adversary force and the nuclear plant security force. During the inspection, the adversary force attempts to reach and damage key safety systems and components while battling the plant's security force. These key safety systems and components protect the reactor core and the spent nuclear fuel pool, both of which contain radioactive fuel. For that reason, it is essential to protect these systems and components from being reached by the adversary force to avoid the potential for radiological release.

Along with the facility's security personnel, many organizations participate in and observe force-on-force inspections. These organizations include Federal, State, and local law enforcement

Onsite security personnel monitor a vehicle access point.

agencies. In addition, emergency planning officials, plant operators, and NRC personnel are present.

Before September 11, 2001, the NRC conducted this type of security inspection at each of the 64 plant sites roughly once every 8 years. Now, the NRC conducts a force-on-force inspection at each plant site at least once every 3 years. The NRC uses lessons learned from previous force-on-force inspections in making changes to its procedures and inspector training.

The current force-on-force program significantly increases the level of authenticity of the inspection, while ensuring the safety of plant employees and the public. The force-on-force inspections involve two sets of security officers. One set maintains the plant's security, while the other set participates in the inspection. In addition, a separate group controls and monitors the inspection. In preparation for a force-on-force inspection, information from tabletop drills, other inspections, and security plan reviews is compiled. This information is then used to design a number of mock commando-style attacks seeking to probe for potential deficiencies in the defensive strategy. Any potentially significant deficiencies in the protective strategy identified during a force-on-force inspection are promptly reviewed and addressed before the NRC inspectors leave the site.

Active-duty U.S. Special Operations Forces advise the NRC inspection teams that conduct force-on-force inspections. These individuals participate in the inspections by helping the NRC inspectors develop the scenarios, providing expert technical advice to the Composite Adversary Force (CAF), assisting the NRC inspectors in evaluating site security forces and systems, and providing an independent evaluation of CAF performance.

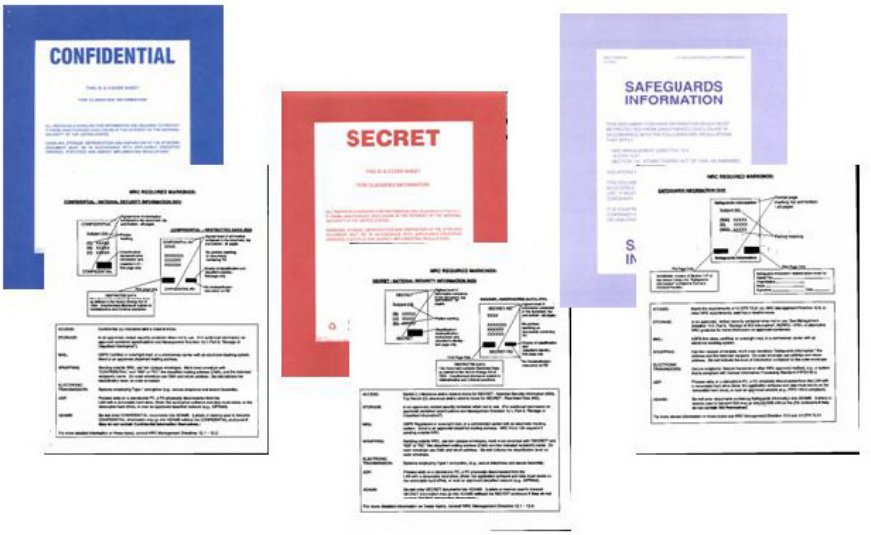
The CAF is a credible, well-trained, and consistent mock adversary force that is vital to the NRC's force-on-force program. The NRC worked with the nuclear industry to develop a CAF trained to NRC standards. The new adversary force has been used for all force-on-force inspections since October 2004 and represents a significant improvement in ability, consistency, and effectiveness. The NRC uses rigorous performance standards to evaluate the CAF at each inspection.

A company that provides security for some U.S. nuclear power plants

also manages the CAF. The NRC recognizes that there may be a perceived conflict of interest, which could result in the appearance that the management company could be unable to objectively test either the CAF or the plant security force. For that reason, the NRC assured that there was a clear separation of functions between the CAF and the plant security force by ensuring an independent, reliable, and credible mock adversary force. As an additional precaution, no member of the CAF may participate in an inspection at his or her home site.

It is important to emphasize that the NRC designs, runs, and evaluates the results of the force-on-force inspections. The mock adversary force does not establish the inspection objectives, boundaries, or timelines. The NRC controls the exercise. To date, the performance of the CAF has been exceptional. No instances of a possible conflict of interest have occurred.

Information Security



The NRC's information security program protects classified, Safeguards Information (SGI), and other sensitive information from unauthorized disclosure. Only those with the appropriate security clearance and a need to know can view such information. The NRC grants facility and security clearances to appropriate individuals at power plants and Category I fuel cycle facilities. These clearances provide licensees with access to classified information. The NRC has also developed comprehensive classification guides. This assures there is consistent and well understood guidance on how to classify this type of information.

The NRC has a long history of promoting openness and transparency in its regulatory and decisionmaking processes. The NRC is dedicated to sharing information among organizations and licensees to enhance prevention and response activities to terrorist and other security incidents. However, the NRC remains diligent in controlling sensitive information to prevent terrorists from potentially gaining access. Consequently, the NRC must balance its commitment to openness with the need to prevent releases of sensitive information.

Using secure transmission equipment, the NRC can rapidly commu-

nicate classified and sensitive unclassified information among NRC Headquarters, regional offices, and licensees. Since September 11, 2001, the NRC has established additional secure communication methods with the National Command Authority, U.S. Department of Defense, and other Federal agencies. These secure communications include high-speed faxing, video teleconferencing, voice equipment, and data networks. The NRC continues to assess the information security program for better ways to protect classified and sensitive unclassified information.

Cyber Security

Following the terrorist attacks on September 11, 2001, the NRC conducted a thorough review of security requirements. Although these attacks did not have a cyber component, the NRC included cyber-security threat and vulnerability assessments in its review. Cyber security is a growing issue across the Nation. To address these concerns, the NRC issued a series of advisories and orders requiring nuclear power plants to take certain actions, including enhancing the protection of their computer systems. Since that time, the NRC has replaced those interim measures with regulations. The NRC added a cyber-security threat component to the DBT in 2007. In 2009, the NRC issued cyber-security requirements under Title 10 of the *Code of Federal Regulations* (10 CFR) Section 73.54, "Protection of Digital Computer and Communication Systems and Networks."

The NRC also recognized the potential security issues associated with digital upgrades and instructed all operating power reactor licensees to enhance access authorization requirements. Recent changes to the regulations have codified these measures. The NRC has also developed regulatory guidance to aid in the secure use of computers in nuclear digital safety systems. This guidance describes how licensees should address potential security vulnerabilities in each phase of the life cycle of the digital safety system. This guidance, in conjunction with industry guidance for digital safety system designs, will help ensure security against cyber vulnerabilities.

Historically, digital computer systems have played a limited role in the operation of U.S. commercial nuclear power plants. Computer systems that help nuclear power plants operate and that control power reactor safety equipment are isolated from the Internet to protect against outside intrusion. However, computer systems are being used in new ways to help maximize plant productivity. These new applications include the following:

- reactor monitoring;
- system operations;

- equipment design and testing;
- recordkeeping;
- maintenance;
- planning; and
- work scheduling.

Many plant computer systems are now linked to digital networks that extend across the plant and, in many cases, are connected to large and diverse corporate networks.

Cyber-security risks are increasing with the expanding use and connectivity of plant-based computer systems. New domestic and international adversaries are emerging, as are new tools that these adversaries can use to exploit potentially vulnerable systems. Because of these developments, there is a growing need to address these risks systematically. The NRC is working with its Federal partners to address the complicated issue of cyber security (e.g., emerging issues associated with the Nation's electrical grid).

Transportation Security

About 300 million shipments of hazardous material are transported by road, rail, or water in the United States each year. Of those shipments, only about 3 million involve radioactive material, most of which is low-level radioactive material. Fewer than 50 shipments contain spent nuclear fuel from commercial nuclear power plants. Since 1979, more than 1,400 shipments of spent nuclear fuel have been successfully transported in NRC-approved packages safely and securely.

NRC requires robust security measures when shipments of spent nuclear fuel or significant quantities of radioactive material are transported.

For decades, the NRC has required spent nuclear fuel packages to withstand different types of accidents, including dropping, puncturing, flooding, and fire. Security measures complement these safety controls. For example, the NRC requires licensees and carriers involved in these shipments to follow approved routes and to provide armed escorts, immobilization devices, and redundant communications. The NRC and those States that the transport will pass through are notified in advance of the shipments.

Stationary portal monitors are used to survey the contents of vehicles entering and exiting nuclear power plants.

For more than 30 years, spent nuclear fuel has been transported under stringent security requirements. However, after the September 11, 2001, terrorist attacks, the NRC reviewed its transportation security program. Following that review, the NRC required security enhancements for shipments of both spent nuclear fuel and significant quan-

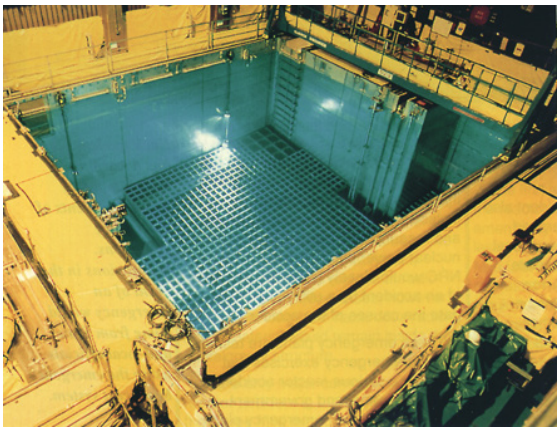
tities of radioactive material. These enhancements include the following:

- preplanning, coordination, and advance notice of shipments;
- additional monitoring of shipments; and
- verification of the trustworthiness of people with information about the shipments.

The NRC also adjusted the security measures for shipments to reflect changes in the DHS Homeland Security Advisory System threat level. During periods of heightened security, the NRC can issue specific advisories to enhance security. These advisories include suspending spent nuclear fuel shipments and requesting that licensees defer shipments of significant quantities of radioactive material.

In addition, the NRC works with other Federal agencies, including DHS, the U.S. Department of Transportation, and DOE, to ensure transportation security.

Spent Nuclear Fuel Storage



The NRC has implemented additional requirements to ensure the safe operation and security of spent fuel pools.

Spent nuclear fuel refers to fuel at commercial nuclear reactors, which is no longer producing enough energy to sustain a nuclear reaction. Periodically, approximately one-third of the nuclear fuel in an operating reactor needs to be unloaded and replaced with fresh fuel.

Spent nuclear fuel is safely stored in specially designed pools at individual reactor sites around the country. Spent fuel pools are strong structures constructed of very thick steel-reinforced concrete walls with stainless steel liners located inside protected areas. Many fuel pools are located below ground level, are shielded by other structures, and have intervening walls that would obstruct a large impact, such as an aircraft impact. NRC has ordered licensees to develop guidance and strategies to maintain and restore spent fuel pool cooling using existing or available resources if cooling is lost for any reason. For many events, plant operators would have significant time to correct a problem or implement fixes to restore cooling.

The NRC has also authorized nuclear power plant licensees to store spent nuclear fuel at reactor sites in NRC-approved dry storage casks. Beginning in the 1980s, the nuclear industry began storing spent nuclear fuel on site in storage casks called independent spent

Independent spent fuel storage installations are used to safely store spent fuel.

fuel storage installations (ISFSIs). These casks are robust, massive concrete and steel structures. These casks provide the same level of safety and security as the spent fuel pools, but can provide additional space for reactors with space limitations in their spent fuel pools.

The NRC has always required ISFSIs to have an onsite physical security system to protect against any unauthorized access to the spent nuclear fuel and its storage area. Additionally, the NRC responded to the September 11, 2001, terrorist attacks by developing new security measures requiring enhanced security at ISFSIs. The NRC also initiated vulnerability assessments of several cask designs used at dry storage ISFSIs. These assessments included aircraft impacts and ground assaults consistent with the DBT. The results of these assessments provide high assurance that all approved cask systems can securely store and protect spent nuclear fuel.

In parallel with these efforts, the NRC worked with the industry to develop guidance for implementing these security measures. After completing the vulnerability assessments, the NRC began an effort to update ISFSI security requirements. As a result of the vulnerability assessments and other lessons learned since September 11, 2001, the NRC issued new inspection procedures in 2008.

The NRC has begun to develop regulations for ISFSIs to incorporate the security measures issued after September 11, 2001. The agency will encourage members of the public to provide comments during the development of the new rules. In addition, the NRC is continuing to evaluate whether changes in adversary capabilities could significantly affect ISFSI security. The NRC is engaging with other Government agencies, the intelligence community, and national laboratories in this task.

Materials Security

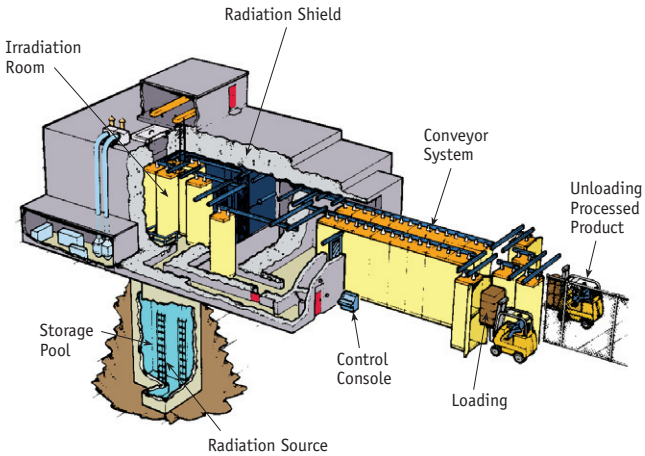
Nuclear and radioactive materials are used in many beneficial ways in the areas of medicine, academia, and industry. However, some materials, if misused, can potentially have negative effects on people and the environment. For these reasons, the NRC regulates the use and handling of certain radioactive materials in the United States.

A radioactive source and a source monitor.

The NRC has longstanding regulatory programs to ensure the security of the materials that it licenses. These programs provide the greatest protection to those materials that could be used in harmful ways if not protected. As a result, the NRC requires licensees to apply a graded level of physical protection and material control and accounting, depending on the material and the relative potential consequences if misused.

After the terrorist attacks on September 11, 2001, the NRC concluded that there was a need to improve the security of nuclear and radioactive materials. The Commission, in conjunction with Agreement States, substantially increased requirements designed to provide reasonable assurance for preventing the theft or diversion of quantities of certain materials. The provisions address background checks, finger-

Commercial Gamma Irradiator



printing, access controls, physical security during use of materials, and physical security during the transportation of quantities of certain materials. Those requirements identified areas to enhance security against terrorist threats. In doing so, the NRC now has an integrated and comprehensive program in place for the management and control of nuclear and radioactive materials.

Since 2007, the NRC and the Organization of Agreement States have been coordinating with the DHS Domestic Nuclear Detection Office and the DOE National Nuclear Security Administration to enhance security measures for self-contained irradiators that contain cesium chloride sources. These irradiators are used for a variety of applications in medical research and industrial activities. The agencies are working with irradiator manufacturers to develop low-cost, easily implemented modifications to further harden these devices against unauthorized access to the source. This voluntary program is meant to enhance the NRC or Agreement State increased control requirements for these irradiators and the facilities where they are used.

In 2009, the NRC implemented a database called the National Source Tracking System (NSTS), which enhances accountability for certain radioactive sources that pose the greatest safety and security concerns. Until the NSTS was deployed, the NRC and its partners performed annual inventories of these sources. The NRC developed the NSTS in conjunction with Federal, State, and international partners. The NSTS requires licensees to report the manufacture, transfer, receipt, disassembly, and disposal of nationally tracked radioactive sources. The NSTS is an important component of the NRC's effort to enhance the accountability and security of radioactive sources.

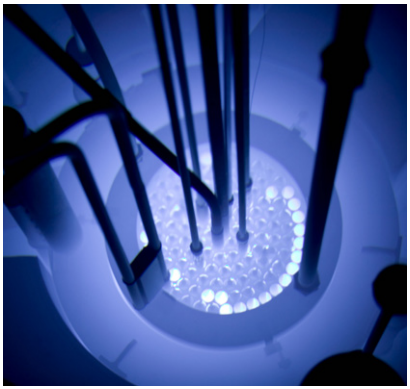
Research and Test Reactors

Research and test reactors (RTRs) pose significantly less risk of radiological exposure to the public than do power reactors. Consequently, the NRC has tailored the security requirements and oversight for RTRs to be consistent with those lower risks. However, following the terrorist attacks of September 11, 2001, the NRC advised RTR licensees to consider certain enhanced security measures to further protect against radiological sabotage and theft of nuclear fuel.

The NRC works with the RTR community to improve security by evaluating if there are potential vulnerabilities that warrant additional preventive or mitigating measures. The NRC takes into consideration the following two main factors in establishing additional security measures for RTRs:

(1) The small radioactive quantity and low potential radiological consequences make it unlikely that a terrorist attack could compromise public health and safety.

(2) Each licensee implements site-specific security plans because each RTR facility is unique in design, operation, use, and location.



The NRC regulates 32 research and test reactors nationwide.

The NRC's security requirements for RTRs implement a graded approach based on the size of each reactor.

The NRC also works with licensees and DOE to evaluate steps to reduce the inventories of reactor fuel at RTRs. This includes converting those reactors using highly enriched uranium to low-enriched uranium through the DOE Global Threat Reduction Initiative. Additionally, DOE is leading a pilot program that includes interagency site visits to RTRs. These visits are followed by a voluntary collaborative agreement to enhance security beyond regulatory requirements.

New Reactors

Although a new nuclear power plant has not been constructed in the United States in many years, interest is growing in expanding domestic nuclear power. In recent years, the NRC has received a number of applications for new reactors and expects to receive more in the future. The NRC is also reviewing new reactor designs.

Next generation nuclear power plants contain features that will make them inherently safer and more secure.

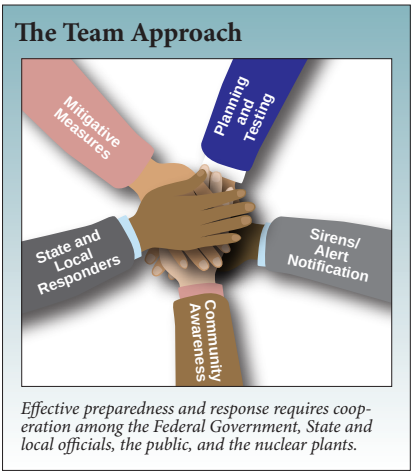
The new reactors will be based on the new NRC-approved designs. These "next-generation" nuclear plant designs have benefited from the current plants' decades of operating experience. The new designs are inherently safer and more secure. They will use many passive systems, thus further ensuring safety with limited reactor operator action.

Also, the Commission has recently approved changes to the regulation of new nuclear power plants and new reactor designs. These changes require applicants for building new power reactors and new reactor design approvals to perform a design-specific assessment of the effects of the impact of a large, commercial aircraft. Although the NRC has defined an aircraft impact as a beyond-design-basis event, new reactors incorporating these changes will be inherently more robust against aircraft impacts.

DHS has the authority and responsibility for a unified national effort to secure the United States by preventing, deterring, and responding to terrorist attacks and other threats and hazards to the Nation. Therefore, the NRC consults with DHS about the potential vulnerabilities of a proposed facility's location to a terrorist threat. This will allow licensees to include appropriate design features and security programs to be implemented to mitigate any potential vulnerability.

Emergency Preparedness

For over 30 years, the NRC has provided regulatory oversight for emergency planning and incident response for all licensees. Commercial nuclear power plants are required to conduct a full-scale exercise involving Federal, State, and local agencies at least once every 2 years. The NRC and FEMA evaluate these exercises to ensure that emergency preparedness programs and the skills of the emergency responders remain effective and to identify and correct any weaknesses. The NRC assesses the onsite response, whereas FEMA assesses the offsite response. In the years between exercises, licensees conduct unevaluated drills and implement lessons learned from previous drills.



Effective preparedness and response requires cooperation among the Federal Government, State and local officials, the public, and the nuclear plants.

After September 11, 2001, the NRC required nuclear power plant licensees to enhance their emergency preparedness, by doing the following:

- identify alternate emergency response facilities;
- notify the NRC promptly during security events;
- develop security-based emergency classification levels and emergency action levels; and
- establish onsite personnel protective actions.

These new measures were promptly put in place, tested through drills and exercises, and verified by the NRC through inspections.

The NRC has also conducted a formal review of the emergency preparedness planning basis to ensure that it will adequately protect the health and safety of the public in light of the current threat environment. The evaluation found that emergency preparedness at nuclear power plants remains strong but could be improved in such areas as communications, resource management, drill programs, and NRC guidance. The

NRC recently published proposed new requirements to include these improvements.

Before 2001, only a few emergency preparedness exercises simulated hostile actions against a nuclear power plant site. A hostile action is an act that uses violent force in an attempt to destroy equipment, take hostages, or intimidate the licensee to achieve an end. Even though the radiological consequences will be the same whether caused by a hostile action or a safety event, hostile actions would provide unique challenges for emergency responders. To prepare for these challenges, the nuclear industry has begun conducting voluntary drills that use scenarios based on hostile actions as initiating events. These drills demonstrate the licensee's ability to coordinate onsite security, operations, and emergency response personnel with offsite organizations, such as State and local emergency management and law enforcement. As part of a proposed rulemaking for 2010, the NRC will incorporate lessons learned from this important industry initiative into the existing emergency preparedness program.

NRC Incident Response

The NRC responds to any incident associated with a U.S. nuclear power plant, RTR, fuel cycle facility, or nuclear materials licensee. The NRC regularly provides support to other Federal, State, and local response agencies during major events such as hurricanes, floods, and wildfires. The NRC coordinates its response actions with other agencies through the use of NRC guidance and consistent with the Federal National Response Framework (NRF).

Chairman Gregory B. Jaczko discusses possible incident response actions with the members of the executive team during an emergency preparedness exercise.

Headquarters Operations Center

The NRC directs its response to events from the Headquarters Operations Center. The operations center is staffed 24 hours a day, 7 days a week with two Headquarters operations officers who have the experience and knowledge to evaluate reported events and to take the proper actions. These actions may include informing NRC management, the agency's Federal partners, licensees, and the media. Since September 11, 2001, the NRC has added staff to the Headquarters Operations Center; improved procedures; and upgraded equipment, including the following:

- upgraded satellite phones;
- new display systems;
- improved computer systems; and
- secure video teleconferencing systems.

An alternate incident response center exists to continue the work of the Headquarters Operations Center in case the Headquarters facility is lost. Each of the NRC's four regions also has incident response centers, which have all been upgraded. These upgrades have added space and improved communications capabilities.

Continuity of Operations

The NRC has a continuity of operations plan (COOP) to ensure that it will continue to operate after a major event that disrupts normal operations. In recent years, the NRC has upgraded and tested its COOP site and has participated in national-level COOP exercises. The

NRC exercises its COOP capabilities to prepare for potential terrorist attacks or other incidents that could disrupt operations. In addition, the COOP addresses agency functions in the event of a flu pandemic. The NRC's COOP is under review regularly and is updated based on the lessons learned during exercises.

Interagency Response

The NRC works with other Federal agencies to improve its response to both nuclear and security emergencies. A law passed in 2002 assigned DHS the task of coordinating the Federal response to domestic incidents. The NRF describes this process. Using the NRF, the NRC will work with local, State, and Federal agencies in both the prevention of, and response to, a potential terrorist event. The NRC has a proven history of providing resources to its partners during exercises and actual events and will continue to work with other Federal agencies to implement the NRF.

The National Infrastructure Protection Plan (NIPP) issued by DHS also contains guidance for the coordination among Federal agencies. The NIPP facilitates information sharing and provides for a coordinated, comprehensive response to threats and events. In addition, the NIPP gives an integrated approach to the roles and responsibilities of Federal, State, local, Tribal, and private sector security partners in protecting critical infrastructure and key resources. Furthermore, the NIPP sets national priorities, goals, and requirements for effective distribution of funding and resources to help ensure that the U.S. Government, economy, and public services continue in the event of natural or man-made disasters.

The NRC supports Federal interagency exercises, such as the National Level Exercises. These exercises reflect an "all-hazards" approach to the Nation's emergency response efforts. Thus, scenarios can be used that potentially involve simulated weapons of mass destruction, major storms, or terrorist attacks. Participating in these exercises provides the NRC with valuable feedback to enhance its own response program.

Another example of interagency coordination is the DHS-led Comprehensive Review Program of commercial nuclear reactors and associated spent nuclear fuel storage facilities. This review was completed in 2007 and identified strengths and potential areas for improvement in the Nation's critical infrastructure and key resources. The NRC continues to work with industry and DHS to assure progress is made on addressing any notable improvement areas.

International Safety and Security of Radiological Sources

Before the terrorist attacks on September 11, 2001, the use of most radiological sources was of concern primarily from a health and safety viewpoint. The NRC authorized exports and imports of sealed sources and bulk material under a "general license" process. Beginning in 2000, the International Atomic Energy Agency (IAEA) Member States began the development of the "Code of Conduct on the Safety and Security of Radioactive Sources" (the IAEA Code of Conduct).

From left to right: Commissioner Kristine L. Svinicki, former Chairman Dale E. Klein, and the Executive Director for Operations R. William Borchardt at the International Atomic Energy Agency in Vienna, Austria.

In 2003, the NRC staff joined with international and domestic partners to discuss with manufacturers of radioactive sources and devices possible ways to make high-risk radioactive sources more secure and less vulnerable to use by persons with malicious intent. The NRC also met with manufacturers to discuss improved methods for use in verifying the legitimacy of purchases of radioactive sources to ensure that these sources are only given to authorized users. Discussions also addressed concerns for ensuring the safe return and disposal of spent radioactive sources.

The NRC worked with the international community and identified 16 radionuclides of concern. These particular sources represent the highest risk for use by a terrorist. The NRC also coordinated with Agreement States to ensure consistency between domestic and international programs, thus providing the supporting technical basis for the IAEA Code of Conduct. The IAEA published the final version of its Code of Conduct, which is not legally binding on IAEA Member States, in 2004.

In 2005, the Commission implemented a rule with enhanced controls over the import and export

of radioactive sources. Under the new rule, licensees must now apply for specific licenses. They also are required to document that the end user is authorized to possess the material and must provide prior notice of shipments. For the export of high-risk sources, the NRC assesses and makes a determination on whether the importing country's regulatory infrastructure is sufficient to maintain adequate control over the material. In countries without adequate regulatory controls, the IAEA Code of Conduct provides for "exceptional circumstances" under which high-risk sources can be exported with additional conditions imposed on the licensee.

The NRC continues to support the development of international standards for implementing the recommendations of the IAEA Code of Conduct for the import and export of radioactive sources. This guidance is intended to balance the needs of international cooperation and commerce without affecting safety and security.

Conclusion

Protecting the Nation's nuclear facilities and materials is a top priority of the NRC. In response to the attacks of September 11, 2001, the NRC moved aggressively to strengthen safety and security throughout the commercial nuclear industry. Working closely with its partners, the NRC will continue to significantly enhance security and emergency preparedness.

Glossary

Agreement State

A State that has signed an agreement with the U.S. Nuclear Regulatory Commission (NRC) under which the State regulates the use of byproduct, source, and small quantities of special nuclear material in that State.

Category I Fuel Cycle Facilities

Fuel cycle facilities that possess more than 5,000 grams of uranium-235 and/or more than 2,000 grams of plutonium.

Classified Information

The two primary types of classified information at the NRC and NRC-regulated facilities are the following:

National Security Information (NSI): Information classified by an Executive Order, whose compromise would cause some degree of damage to national security.

Restricted Data (RD): Information classified by the Atomic Energy Act, whose compromise would assist in the design, manufacture, or utilization of nuclear weapons.

The lowest level of classified information is Confidential; the next higher is Secret, and the highest is Top Secret. Confidential and Secret information will also be either NSI or RD. Access to classified information requires a personnel security clearance equal to or higher than the level of information and a need to know.

Composite Adversary Force

A credible, well-trained, and consistent mock adversary force used in force-on-force exercises.

Design-Basis Threat

A profile of the type, composition, and capabilities of a possible adversary. The NRC and certain licensees use the design-basis threat as a basis for designing safeguards systems to protect against acts of radiological sabotage and to prevent the theft of special nuclear material. This term is applied to clearly identify for a licensee the expected capability of its facility to withstand a threat.

Emergency Preparedness

Action taken to be ready for emergencies before they happen. The objective of emergency preparedness is to simplify decisionmaking during emergencies.

The emergency preparedness process incorporates the means to rapidly identify, evaluate, and react to a wide spectrum of emergency conditions.

High-Level Waste

Radioactive materials at the end of a useful life cycle that should be properly disposed of, including the following:

- highly radioactive material from the reprocessing of spent nuclear fuel, including liquid waste directly in reprocessing and any solid material derived from such liquid waste that contains fission products in concentrations;
- irradiated reactor fuel; and
- other highly radioactive material that the Commission, consistent with existing law, determines by rule to require permanent isolation.

With respect to NRC licensees, high-level waste is primarily in the form of spent fuel discharged from commercial nuclear power reactors.

Hostile Action

An act toward a nuclear power plant or radioactive material facility or its personnel that includes the use of violent force to destroy equipment, take hostages, and/or intimidate the licensee to achieve an end. This includes an attack by air, land, or water that uses guns, explosives, projectiles, vehicles, or other devices to deliver destructive force. Other acts that satisfy the overall intent may be included.

Licensed Material

Source material, special nuclear material, or byproduct material received, possessed, used, transferred, or disposed of under a general or specific license issued by the NRC.

Licensee

An entity or individual licensed by the NRC to conduct the following activities:

- construction, operation, and decommissioning of commercial reactors and fuel cycle facilities;
- possessing, using, processing, exporting, importing, and certain aspects of transporting nuclear materials and waste; and
- siting, design, construction, operations, and closure of waste disposal sites.

NRC Headquarters Operations Center

The NRC Headquarters Operations Center in Rockville, MD, serves as the focal coordination point for communicating with NRC licensees, State agencies, and other Federal agencies about operating events in both the nuclear reactor and nuclear materials industry. Headquarters operations officers, who are trained to receive, evaluate, and respond to reported events, staff the Headquarters Operations Center 24 hours a day, 7 days a week.

Nuclear Energy

The energy liberated by a nuclear reaction (fission or fusion) or by radioactive decay.

Nuclear Power Plant

An electrical generating facility that uses a nuclear reactor as its heat source to provide steam to a turbine generator.

Nuclear Waste

A particular type of radioactive waste that is produced as part of the nuclear fuel cycle (i.e., those activities needed to produce nuclear fission or the splitting of the atom). These activities include the extraction of uranium from ore, the concentration of the extracted uranium, the processing of the concentrated uranium into nuclear fuel, and the disposal of byproducts. "Radioactive waste" is a broader term that includes all waste that contains radioactivity. Residues from water treatment, contaminated equipment from oil drilling, and tailings from the processing of metals such as vanadium and copper also contain radioactivity but are not "nuclear waste" because they are produced outside of the nuclear fuel cycle. The NRC generally regulates only those wastes produced in the nuclear fuel cycle (e.g., uranium mill tailings, depleted uranium, and spent fuel rods).

Radionuclide

An unstable isotope of an element that emits radiation as it decays or disintegrates spontaneously.

Safeguards

The use of material control and accounting programs, physical protection equipment, and security forces to verify that all special nuclear material is properly controlled and accounted for. As used by the International Atomic Energy Agency, verification that the "peaceful use" commitments made in binding nonproliferation agreements, both bilateral and multilateral, are honored.

Safeguards Information

Safeguards Information (SGI) is a special category of sensitive unclassified information authorized by Section 147 of the Atomic Energy Act to be protected. Safeguards information concerns the physical protection of operating power reactors, spent fuel shipments, strategic special nuclear material, or other radioactive material.

While SGI is considered to be sensitive unclassified information, its handling and protection more closely resemble the handling of classified Confidential information rather than other sensitive unclassified information.

The categories of individuals who are permitted access to SGI are listed in Title 10 of the Code of Federal Regulations (10 CFR) 73.21, "Protection of Safeguards Information: Performance Requirements," 10 CFR 73.22, "Protection of Safeguards Information: Specific Requirements," and 10 CFR 73.23, "Protection of Safeguards Information—Modified Handling: Specific Requirements."

Sensitive Unclassified Non-Safeguards Information

Sensitive Unclassified Non-Safeguards Information (SUNSI) is information that is generally not publicly available and encompasses a wide variety of categories (e.g., personnel privacy, attorney-client privilege, confidential source, etc.).

Information about a licensee's or applicant's physical protection or material control and accounting program for special nuclear material not otherwise designated as Safeguards Information or classified as National Security Information or Restricted Data is required by Title 10 of the Code of Federal Regulations (10 CFR) 2.390, "Public inspections, exemptions, requests for withholding," to be protected in the same manner as commercial or financial information, in other words, they are exempt from public disclosure. SUNSI policy and procedures are the responsibility of the Office of Information Services at the NRC.

Special Nuclear Material

Plutonium, uranium-233, or uranium enriched in the uranium-233 or uranium-235 isotopes.

Spent Fuel Pool

An underwater storage and cooling facility for spent (used) fuel elements that have been removed from a reactor.

List of Acronyms

CAF	Composite Adversary Force
COOP	continuity of operations plan
DBT	design-basis threat
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
FEMA	Federal Emergency Management Agency
IAEA	International Atomic Energy Agency
ISFSI	independent spent fuel storage installation
NIPP	National Infrastructure Protection Plan
NRC	U.S. Nuclear Regulatory Commission
NRF	National Response Framework
NSIR	Office of Nuclear Security and Incident Response
NSTS	National Source Tracking System
RTR	research and test reactor
SGI	Safeguards Information
SUNSI	Sensitive Unclassified Non-Safeguards Information

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at NRC's Public Electronic Reading Room at http://www.nrc.gov/reading-rm.html.
Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and *Title 10, Energy*, in the Code of *Federal Regulations* may also be purchased from one of these two sources.

1. The Superintendent of Documents
   U.S. Government Printing Office
   Mail Stop SSOP
   Washington, DC 20402–0001
   Internet: bookstore.gpo.gov
   Telephone: 202-512-1800
   Fax: 202-512-2250
2. The National Technical Information Service
   Springfield, VA 22161–0002
   www.ntis.gov
   1–800–553–6847 or, locally, 703–605–6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:
Address: U.S. Nuclear Regulatory Commission
Office of Administration
Mail, Distribution and Messenger Team
Washington, DC 20555-0001
E-mail: DISTRIBUTION@nrc.gov
Facsimile: 301–415–2289

Some publications in the NUREG series that are posted at NRC's Web site address http://www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, and transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—
The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852–2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—
American National Standards Institute
11 West 42nd Street
New York, NY 10036–8002
www.ansi.org
212–642–4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor-prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR–XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX), (4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG–0750).

NUREG/BR-0314, Rev. 1

September 2009