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

ACKNOWLEDGMENTS

Jared Justice

Carolyn Kahler

Kim Lawson-Jenkins

Curtis Newkirk

Rebecca Stone

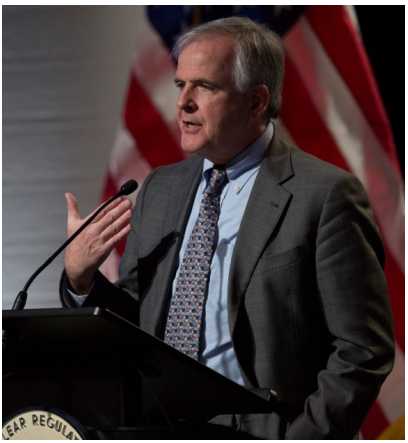
Adam Tucker

Brian Zaleski

TABLE OF CONTENTS

FOREWORD FROM THE CHAIRMAN

On January 8, 2015, the U.S. Nuclear Regulatory Commission (NRC) marked its 40th anniversary. This significant milestone created an opportunity to reflect on the many ways the agency and its regulatory program have evolved over the past four decades and those seminal moments in our history that provided the impetus for change. From the beginning, the NRC understood that



Chairman Stephen G. Burns speaks during the Regulatory Information Conference at NRC Headquarters

its mission of ensuring the safe use of radioactive materials for beneficial civilian purposes included assessing and planning for emergency events. In 1979, the accident at the Three Mile Island nuclear plant in Pennsylvania provided industry and the NRC with new insights, which the NRC used to reevaluate its assumptions and approaches to emergency preparedness. These insights are still reflected in our regulatory program today.

Lessons learned from the terrorist attacks of September 11, 2001, prompted the NRC to enhance its regulatory program to meet the security and emergency preparedness challenges of the new threat environment. Earlier editions of "Protecting Our Nation" have described these efforts, including revising the design basis threat regulations in Title 10 of the Code of Federal Regulations (10 CFR) Part 73 in 2007 to ensure that nuclear power plants and other licensed facilities continue to have effective security measures in place. More recently, in 2013, the NRC published a new rule in 10 CFR Part 37, which imposes security requirements for the most risk-significant radioactive material that are intended to protect against the theft or diversion of this material.

Our efforts to meet the challenges of the threat environment have gone beyond the physical protection of radioactive material. The technological advances of the last few decades that have led us into the digital age have brought with them new threats to the protection of digital equipment and information. The NRC has made significant efforts to address these threats and to improve oversight for the protection of critical digital assets

at nuclear power plants. In March 2009, many of these efforts culminated in the NRC's publication of the cyber security rule, which applies to power reactor licensees and combined license applicants. More recently, in 2013, the NRC established a Cyber Security Directorate to centralize the agency's oversight in this area.

If a reflection on the agency's history teaches us anything, it is that change is constant. The NRC is committed to planning for and responding to change in order to ensure the protection of public health and safety and the common defense and security. I hope you find that this latest edition of "Protecting Our Nation" provides an informative description of the NRC's current safety and security activities.

Stephen G. Burns

Chairman, NRC

EXECUTIVE SUMMARY

For more than 40 years, the NRC has maintained effective programs for nuclear security, emergency preparedness, and incident response as part of the agency's overall mission to protect people and the environment.

The NRC requires safe and secure operations at all licensed nuclear facilities and in the use of radioactive materials. "Safety" refers to operating each facility in a way that protects the public's health and safety and the environment. "Security" refers to protecting each facility from threats to steal or divert special nuclear material or to commit radiological sabotage. Both safety and security rely on people, programs, and equipment to make sure NRC requirements are properly implemented. Safety and security at licensed nuclear facilities are achieved in layers, with multiple approaches at work to ensure licensed activities do not result in an unreasonable risk to public health and safety. For example, nuclear power reactors are safe, robust structures designed and built to withstand hurricanes, tornadoes, floods, and earthquakes. In addition, the security of operating reactors is maintained through a well-trained and armed security force, physical barriers, access controls, and intrusion detection, assessment, and surveillance systems.

The coordination of threat information serves as an additional layer of protection. The NRC works closely with Federal, State, Tribal, and local authorities to help ensure threat information is quickly disseminated to licensees to allow an effective response in the event of an attack. Together, these layers of defense provide a level of security that achieves high assurance of protection.

The NRC regulates security, emergency preparedness, and incident response programs at licensed facilities that are mature, robust, and well integrated. Existing programs are maintained and enhanced while new programs are developed, when necessary, to address evolving threats.

From left to right: Commissioner Jeff Baran, Commissioner Kristine L. Svinicki, Chairman Stephen G. Burns, and Commissioner William C. Ostendorff

Major activities covered in this document highlighting both ongoing and recent NRC accomplishments include:

- verifying that licensees have implemented physical and cyber security requirements through licensing reviews and inspections
- using a high level of realism in force-on-force inspections, while ensuring the safety of employees and the public, and continually applying lessons learned from previous years
- ensuring safe and secure transport of spent fuel along NRC approved routes, using NRC-approved packages
- implementing the National Source Tracking System (NSTS) 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
- enhancing physical security requirements for radioactive materials and devices at facilities and in transportation through developing and implementing 10 CFR Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material"
- developing a new physical security inspection program and increasing inspections at decommissioning nuclear reactors
- assessing and sharing threat information to rapidly promote protection of licensed facilities
- supporting the development of international standards
- coordinating activities related to nuclear industry efforts to conduct emergency preparedness exercises with security scenarios ensuring continuous training and improvement to equipment and procedures in the NRC Headquarters Operations Center (HOC) and regional Incident Response Centers (IRCs)

Executive Director for Operations, Mark A. Satorius speaks to NRC stakeholders

NUCLEAR REACTOR SECURITY

Security for Operating, New, and Nonpower Reactors

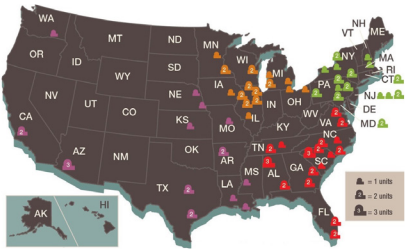
The NRC requires robust security at the Nation's nuclear reactors. To achieve this, each reactor licensee is required by NRC regulation to integrate people, programs, procedures, and equipment to provide "defense in depth" at reactor facilities.

Effective NRC regulations, licensee implementation of these regulations, and strong partnerships with Federal, State, Tribal, and local law enforcement agencies helps ensure effective security at nuclear reactors across the country. At the same time, the agency recognizes the need for continued vigilance given the evolving threat environment.

An NRC-licensed operating nuclear power plant

Operating Reactors

The NRC makes sure the security posture at operating reactors is appropriate and complies with NRC regulations through a variety of licensing, inspection, and enforcement activities. This includes NRC review of any changes or updates sites make to their protective strategy, security plan, or implementing procedures to ensure there is a high assurance of protection against the Design Basis Threat (DBT). The DBT describes the adversary force that the licensee must defend against. The DBT is based on realistic assessments of the tactics, techniques, and procedures used by international and domestic terrorist groups and organizations.



U.S. map with operating nuclear power reactors displayed by the four NRC regions (RI – green; RII – Red; RIII – Orange; RIV – Purple)

One significant component of the security inspection program is force-on-force security inspections.

[1] Design Basis Threat for radiological sabotage is a determined violent external assault, attack by stealth, or deceptive actions, including diversionary actions, by an adversary force capable of operating in each of the following modes: a single group attacking through one entry point, multiple groups attacking through multiple entry points, a combination of one or more groups and one or more individuals attacking through multiple entry points, or individuals attacking through separate entry points, with attributes, assistance and equipment as described in 10 CFR Part 73, "Physical Protection of Plants and Materials."

These inspections assess the licensees' ability to defend its facility against the DBT for radiological sabotage[1] and provide valuable insights that allow the NRC to evaluate and improve the effectiveness of each site's security program.

The comprehensive security regulations for operating reactors also include a cyber security threat component. All operating reactor licensees have cyber security plans that have been reviewed and approved by the NRC. The NRC uses inspections to verify that each operating reactor has implemented the cyber security requirements.

New Reactors

An NRC Resident Inspector at a nuclear power plant construction site discusses inspection activities

The NRC has many programs in place to meet the challenges associated with new reactor design, licensing, and construction. Four new AP1000 reactors are currently under various stages of construction. Watts Bar Unit 2 is also in the final stages of construction.

The "next-generation" nuclear power reactor designs have benefited from the lessons learned over decades of commercial operation with current operating reactors. The new reactor designs are inherently safer and more secure, and are designed to use passive systems to achieve safety with fewer reactor operator actions.

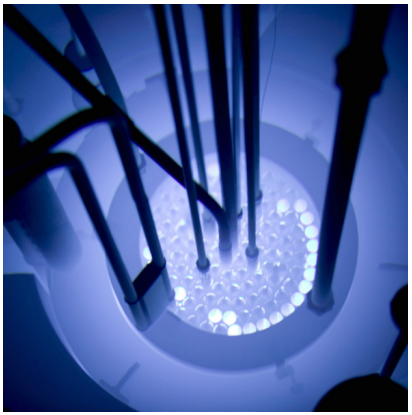
Construction at a nuclear power plant site

New reactors must meet the same safety and security requirements as currently operating reactors. Additionally, as required by Section 657 of the Energy Policy Act of 2005, prior to issuing a license for a new reactor, the NRC consults with the U.S. Department of Homeland Security (DHS) about the potential vulnerabilities of the proposed reactor location to a terrorist threat.

Nonpower Reactors

Nonpower reactors (NPRs) pose significantly less radiological risk to the public than nuclear power reactors due to the presence of a smaller quantity of nuclear material. The nature and form of the material also makes it difficult to disperse or divert. As a result, the NRC has

tailored the security requirements and oversight of these reactors to be commensurate with these lower risks. Recognizing the diverse NPR designs and usages, the NRC works with the NPR community to enhance security by identifying potential vulnerabilities that warrant facility-specific preventive or mitigating measures.



The NRC regulates 31 NPRs nationwide

To further reduce risk, the NRC works with licensees and the U.S. Department of Energy (DOE) to evaluate steps to reduce the inventories of reactor fuel at these sites. This includes converting those reactors using highly-enriched uranium to using low enriched uranium through the DOE's Office of Material Management and Minimization.

Design Basis Threat for Radiological Sabotage

The DBT for radiological sabotage describes the adversary force the nuclear power plant licensee must defend against. It is based on realistic assessments of the tactics, techniques, and procedures used by international and domestic terrorist groups and organizations, as well as cyber criminals. The NRC works with national experts and analyzes classified and other sensitive information to establish this DBT. The NRC also relies on the intelligence community, law enforcement agencies, and Federal, State and local governments to provide accurate and timely information about the capabilities and activities of adversary groups.

Barriers are part of the physical protection system used at operating reactors to defend against the DBT

The NRC staff regularly reviews this DBT against current threat intelligence, both domestic and international, to determine if any changes are needed. The specifics of this DBT are not publicly available in order to protect sensitive security

information. In general, however, each operating reactor licensee establishes the following security strategy:

- cyber security program
- physical security program to include but not limited to:
  - security patrols
  - security posts and physical barriers
  - vehicle and personnel searches
  - training of security and emergency response personnel
  - enhanced weapons systems needed to implement an effective defense-in-depth strategy
  - communication equipment
  - site access controls for personnel, to include more thorough employee background checks

Onsite security personnel conduct vehicle checks before allowing entry to a plant

Security Baseline Inspections

The NRC's operating reactor security baseline inspection program is the primary way the agency verifies that each nuclear power reactor licensee operates the facility according to security regulations. Under the program, security experts from NRC Headquarters and NRC Regional offices in the Philadelphia, Atlanta, Chicago, and Dallas areas carry out security inspections at each facility. Onsite Resident Inspectors, in addition to the security inspectors from Headquarters and the Regional offices, monitor licensees' security-related activities throughout the year. The inspectors provide firsthand, independent assessments of plant conditions and performance. They document their findings in writing, and conduct follow-up inspections to ensure any necessary corrections have been made. Security baseline inspections include the following licensee activities:

An NRC inspector gathers information at a nuclear power plant

- Access Authorization
- Access Control
- Contingency Response Force-on-Force
- Equipment Performance, Testing, and Maintenance
- Protective Strategy Evaluation
- Protection of Safeguards Information (SGI)
- Security Training
- Fitness-for-Duty Program
- Cyber Security
- Materials Control and Accounting
- Target Set Development

A licensee's security program is made up of multiple components that together provide high assurance of adequate protection

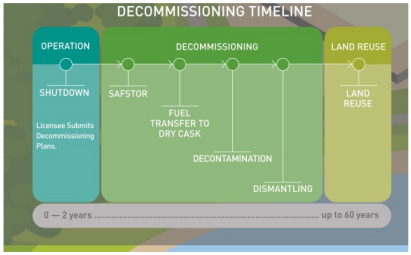
The NRC's overall evaluation of an operating reactor's performance considers the results of all security inspections. At any time, if a significant security issue is identified, the NRC requires the licensee to resolve the issue promptly. If necessary, the NRC can take enforcement action, which may result in civil penalties. Some information related to these inspections is available to the public on the NRC website. Some information is not publicly available because it could potentially aid an adversary.

Decommissioning Reactor Security Core Inspections

The NRC's decommissioning reactor security core inspection program is the primary way the agency verifies that the licensee of each decommissioning nuclear power reactor complies with security regulations. Security experts from NRC Regional offices carry out these inspections. The inspectors provide firsthand, independent assessments of plant conditions and performance, document their findings in writing, and conduct follow-up inspections to ensure any necessary corrections have been made. Security core inspections include the following licensee activities:

- Access Authorization
- Access Control
- Equipment Performance, Testing, and Maintenance
- Protective Strategy Evaluation
- Protection of SGI
- Security Training
- Fitness-for-Duty Program

- Cyber Security
- Materials Control and Accounting
- Review of Decommissioning Reactor Target Sets



The NRC's overall evaluation of a decommissioning reactor's performance considers the results of security core inspections. At any time, if a significant security issue is identified, the NRC requires the licensee to resolve the issue promptly. If necessary, the NRC can take enforcement action, which may result in civil penalties. Some information related to these inspections is available to the public on the NRC website. Some information is not publicly available because it could potentially aid an adversary.

An NRC-licensed facility undergoes decommissioning

Force-on-Force Security Inspections

An essential part of the NRC oversight of nuclear power reactors is the force-on-force security inspection, which is part of the NRC's security baseline inspection program. The NRC has used force-on-force inspections regularly since 1991. Force-on-force inspections assess the ability of the licensee of each nuclear power facility to defend against the DBT for radiological sabotage. They also provide valuable insights that allow the NRC to evaluate the effectiveness of licensee security programs.

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

A full force-on-force inspection spans several weeks and includes both tabletop drills and simulated combat between a mock adversary force and the security force at the operating reactor. During the inspection, the mock adversary force tries to reach and damage key safety systems and components identified as target sets while battling the facility's security force. These key safety systems and components protect the reactor core and the spent fuel pool, both of which may contain radioactive fuel. For that

reason, it is essential to protect these systems and components to avoid the potential for a radiological release.

Licensees are authorized to use deadly force while protecting nuclear facilities from adversaries

Along with the security personnel at the facility, offsite organizations may participate in and/or observe force-on-force inspections. These organizations include Federal, State, and local law enforcement agencies. In addition, emergency planning officials, plant operators, and NRC personnel are present.

By law, the NRC conducts a force-on-force inspection at each nuclear power reactor at least once every 3 years. The NRC incorporates lessons learned from previous force-on-force inspections when making changes to its procedures and inspector training programs. The NRC is implementing changes to these force-on-force inspections based on a lessons-learned review approved by the Commission.

The force-on-force security inspection program is as realistic as possible while also ensuring the safety of the facility employees and the public. The force-on-force inspection involves two shifts of the security officers at the facility: one set maintains the security of the reactor, while the other set participates in the inspection. In addition, a separate group controls and monitors both inspection participants and on-duty security officers during the inspection. The NRC has overall control of the exercise. The NRC inspection team monitors all aspects of the exercise to ensure the safety of the participants and that the exercise is conducted according to NRC inspection standards. In preparation for a force-on-force inspection, NRC security inspectors compile information from tabletop drills, facility tours, and security plan reviews. This information is used to design mock attacks seeking to probe for potential vulnerabilities in the defensive strategy of the facility. Any potentially significant findings identified during a force-on-force inspection are promptly reviewed, addressed, and corrected before the NRC inspectors leave the facility.

Licensees implement multiple layers of defense to demonstrate the effectiveness of their security program during force-on-force training exercises

Active-duty U.S. Special Operations Forces advise the NRC teams that conduct force-on-force inspections. These individuals participate in the inspections by helping the NRC inspectors develop the attack scenarios, providing expert technical advice to the mock adversary force, and assisting the NRC inspectors in evaluating site security forces and systems. They also independently evaluate the mock adversary performance.

The mock adversary is a credible, well trained, and consistent force that is vital to the NRC's force-on-force program. The NRC works with the nuclear industry to develop mock adversary training and uses rigorous performance standards to evaluate the mock adversary force at each inspection.

It is important to note that the NRC designs, runs, and evaluates the force-on-force inspections. The mock adversary force does not establish the inspection's objectives, boundaries, or timelines.

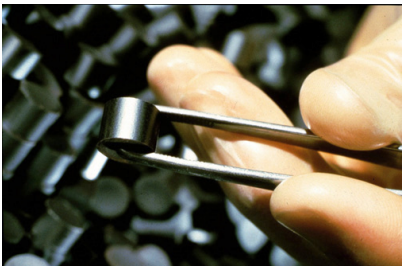
MATERIALS SECURITY

Security for the Use, Storage, and Transportation of Nuclear and Radiological Materials

The NRC has longstanding regulatory programs that ensure the security of materials used at licensed facilities. 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 it is misused. Security programs may include personnel background checks, personnel access controls, security barriers, detection of unauthorized access, and an armed law enforcement response. These programs provide the greatest protection to those materials that could be used in harmful ways if not protected. Given the evolving threat environment, the agency recognizes the need for continued vigilance.

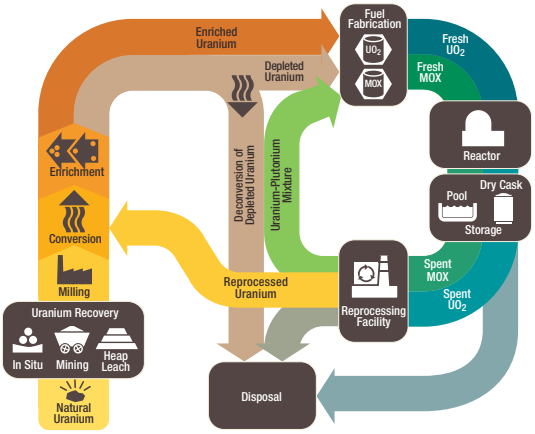
Fuel Cycle Facilities

The NRC licenses and inspects all commercial fuel cycle facilities that manufacture fuel from mined uranium ore for use in nuclear reactors. This



A small ceramic fuel pellet

includes uranium recovery facilities that mill uranium; facilities that convert, enrich, and fabricate the uranium into nuclear fuel for nuclear reactors; and deconversion facilities that will process the depleted uranium for recycling or disposal. The NRC also regulates the fabrication of other types of nuclear fuel, such as mixed oxide fuel, which is a combination of uranium and plutonium oxides.



The stages of the nuclear fuel cycle. Note: The reprocessing of spent nuclear fuel, including mixed-oxide (MOX) fuel, is not practiced in the U.S.

The NRC regulates fuel cycle facilities through a combination of the following:

- safety and security regulations that licensees must meet to obtain and retain a license to use nuclear materials
- authorization for an applicant to use or transport nuclear materials or operate a nuclear facility
- an oversight process that includes inspections, enforcement, assessment of licensee performance, and investigation of reports of wrongdoing
- support activities (e.g., research, hearings, independent reviews)

Additionally, the NRC has issued orders to the licensees of various fuel cycle facilities containing detailed requirements on detecting, assessing, and responding to malicious acts, including enhancing the protection of computer systems. In 2012, the NRC issued a cyber security paper that communicated the staff's approach, or roadmap, to evaluating the need for cyber security requirements for specific types of licensees, including fuel cycle facilities. The roadmap is designed to make sure appropriate cyber security protections are implemented efficiently at all NRC-licensed fuel cycle facilities to protect people and the environment.

Spent Fuel Facilities

Spent nuclear fuel refers to nuclear reactor fuel that has been used to the extent that it can no longer effectively sustain a chain reaction. Periodically, about one third of the nuclear fuel in an operating reactor needs to be replaced with fresh fuel. Spent nuclear fuel is initially stored in specially designed pools of water called spent fuel pools that store and cool the nuclear fuel while the radioactive materials in the fuel decay.
Spent fuel pools are robust structures, constructed of very thick steel-reinforced concrete walls with stainless steel liners, and located

The NRC imposes stringent requirements to ensure the safe and secure operation of spent fuel pools

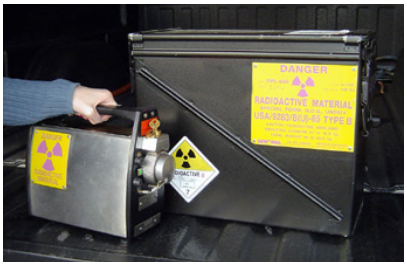
inside protected areas at nuclear power reactor facilities. Many are located below ground level, are shielded by other structures, and have intervening walls that protect the pool and the fuel from a large impact, such as an aircraft. The NRC regulations require licensees to develop strategies and procedures to maintain and restore spent fuel pool cooling if cooling is lost. For many events, plant operators would have significant time to correct a problem or implement fixes to restore cooling.

The NRC also has authorized the storage of spent nuclear fuel in NRC-approved dry storage casks. Beginning in the 1980s, the nuclear industry began storing spent nuclear fuel on site in storage casks located at Independent Spent Fuel Storage Installations (ISFSIs). These casks are robust, massive concrete and steel structures. Spent nuclear fuel is moved from the spent fuel pool into dry cask storage after several years to free space in the spent fuel pool. The NRC conducted security vulnerability assessments of several cask designs used at dry storage ISFSIs. These assessments included aircraft impacts and ground assaults consistent with the DBT. 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. In addition, the NRC continues to evaluate whether changes in adversary capabilities could significantly affect ISFSI security.

Spent fuel is safely and securely stored in an ISFSI

The NRC issued orders to strengthen the security postures at ISFSIs after September 11, 2001, and is currently planning to update regulations to improve the consistency and clarity of the security measures for ISFSIs. The NRC will be seeking comments from members of the public and other stakeholders during the development of the updated regulations.

Byproduct Material



A radiography camera and its approved transport container

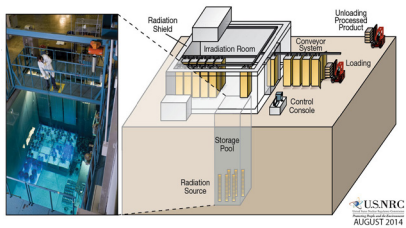
Nuclear and radioactive materials also are used in many beneficial ways in medicine, academia, and industry; however, some materials, if misused, can have negative effects on people and the environment. The terrorist attacks on September 11, 2001, heightened concerns about the use of radioactive materials in an attack, such as a "dirty bomb" attack. After September 11, 2001, the NRC and its Agreement State partners strengthened the security of risk-significant radioactive materials. The NRC and Agreement States issued orders imposing comprehensive security measures appropriate to facilities housing byproduct material and the level of security risk associated with these materials.

The security orders established a multi-layered framework that allows licensees to develop facility-specific

security programs. Key elements of the program include:

- background checks, including fingerprinting, to ensure that people with access to radioactive material are trustworthy and reliable
- personnel access controls to areas where radioactive material is stored or used
- security plans or procedures designed to detect, deter, assess, and respond to unauthorized access attempts
- coordination and response planning between licensees and local law enforcement agencies
- coordination and tracking of shipments of radioactive material
- additional security barriers to discourage theft of portable devices containing radioactive material

In 2013, the NRC published security regulations in a new comprehensive rule titled 10 CFR Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material". The Part 37 rule incorporated and expanded on the requirements from the security orders and included lessons learned from implementing, inspecting, and enforcing the orders. Part 37 also strengthened security requirements for transporting byproduct material. In 2014, compliance with Part 37 was required for NRC licensees and the previous security orders were rescinded. The Agreement States must establish compatible regulations by March 2016 and the security orders will remain in effect for Agreement State licensees until that time.



Commercial irradiators use gamma radiation to eliminate harmful bacteria, germs, and insects in food and medical supplies, and to harden wood flooring. This process does not leave a radioactive residue or make the treated products radioactive

The NRC also developed an Integrated Source Management Portfolio that includes the NSTS, the Web-Based Licensing (WBL) database, and the License Verification System (LVS). The NSTS is a database that enhances accountability for certain radioactive sources that pose the greatest safety and security concerns. The NSTS requires licensees to report the manufacture, transfer, receipt, disassembly, and disposal of radioactive sources that are required to be tracked nationally. The NSTS is an important component of the NRC's effort to enhance the accountability and security of radioactive sources. The WBL was implemented in 2012 and manages the licensing lifecycle from initial application through license issuance, amendment, and

termination. It also modernizes the method for authenticating radioactive material licenses. The NRC uses WBL as its licensing system, and it is available for use by Agreement States for licensing purposes. The LVS was added in 2013. It is a secure, fast, digital system for use by licensees to confirm that another party is properly licensed and authorized to possess radioactive material before shipping or transferring radioactive material to that party.

Transportation

The NRC and the U.S. Department of Transportation (DOT) regulate the transportation of nuclear and radiological materials through a combination of safety and security requirements. About 300 million shipments of hazardous material are transported by road, rail, air, or water in the United States each year. Of those shipments, only about 3 million involve radioactive material, most of which is low-risk radioactive material. Fewer than 50 shipments contain spent nuclear fuel. Spent nuclear fuel has been successfully transported in NRC-approved containers safely and securely since 1979.

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

For decades, the NRC has required radioactive material containers to be designed and manufactured to withstand accidents including dropping, puncturing, flooding, and fire. Security measures complement these safety controls. For example,

The NRC requires licensees and carriers involved in spent nuclear fuel shipments to follow approved routes

the NRC requires licensees and carriers transporting spent nuclear fuel shipments to follow approved routes and to provide armed escorts, vehicle immobilization devices, and redundant communications. In addition, in advance of the transportation of any shipment, each licensee must notify the NRC, States, and as appropriate, federally recognized Tribal Nations.

For more than 30 years, spent nuclear fuel has been transported under stringent security requirements. After the terrorist attacks on September 11, 2001, the NRC reviewed its transportation security program. As a result, the agency began requiring

security enhancements for both shipments of spent nuclear fuel and shipments of significant quantities of radioactive material. These enhancements included the following:

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

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

Effective NRC regulation, licensee implementation of these regulations, and strong partnerships with Federal, State, Tribal, and local authorities have ensured effective security for the storage and transportation of nuclear and radiological materials across the country.

Design Basis Threat for Theft or Diversion[2]

The DBT for theft or diversion describes the adversary force that Category I[3] fuel cycle facilities must defend against. Additionally, these facilities must defend against the DBT for radiological sabotage, as discussed

Security barriers provide one of the many layers of physical protection

in the Design Basis Threat for Radiological Sabotage section. Similar to the DBT for radiological sabotage, the DBT for theft or diversion is based on realistic assessments of the tactics, techniques, and procedures used by international and domestic terrorist groups and organizations, as well as cyber criminals. 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 adversary groups.

[2] Design Basis Threat for theft or diversion of formula quantities of strategic special nuclear material is a determined violent external assault, attack by stealth, or deceptive actions, including diversionary actions, by an adversary force capable of operating in each of the following modes: a single group attacking through one entry point, multiple groups attacking through multiple entry points, a combination of one or more groups and one or individuals attacking through multiple entry points, or individuals attacking through separate entry points, with attributes, assistance and equipment as described in Title 10 CFR Part 73, "Physical Protection of Plants and Materials."

[3] Fuel cycle facilities that possess more than 5,000 grams (about 11 pounds) of strategic special nuclear material (defined as a "formula quantity") or more as computed by the formula, grams = (grams contained U-235) + 2.5 (grams U-233 + grams plutonium) as further described in 10 CFR Part 73, "Physical Protection of Plants and Materials."

Following September 11, 2001, the NRC thoroughly reviewed both DBTs to ensure that the security measures in place at Category I fuel cycle facilities continued to be effective. The NRC issued orders that upgraded the DBTs as a result of this review.

Vehicle barriers are part of the physical protection system used by some nuclear facilities

These orders were later incorporated into a revised DBT rule. The rule reflected insights gained from the latest threat information and included a cyber threat component. The agency also considered, and as appropriate, incorporated the following 12 factors identified in the Energy Policy Act of 2005:

1) The events of September 11, 2001

2) An assessment of physical, cyber, biochemical, and other terrorist threats

3) The potential for attack on facilities by multiple coordinated teams of a large number of individuals

4) The potential for assistance in an attack from several persons employed at the facility

5) The potential for suicide attacks

6) The potential for water-based and air-based threats

7) The potential use of explosive devices of considerable size and other modern weaponry

8) The potential for attacks by persons with a sophisticated knowledge of facility operations

9) The potential for fires, especially fires of long duration

10) The potential for attacks on spent fuel shipments by multiple coordinated teams of a large number of individuals

11) The adequacy of planning to protect the public health and safety at and around nuclear facilities, as appropriate, in the event of a terrorist attack against a nuclear facility

12) The potential for theft or diversion of nuclear material from such facilities

The NRC regularly reviews the DBTs against the current threat intelligence, both domestic and international, to determine whether changes are warranted. Specific characteristics of the DBTs are not public to protect sensitive security information.

Security Core Inspections

The NRC's security core inspection program is the primary way the agency ensures the physical protection

NRC licensees have measures that limit the exposure of security personnel to possible attack, including the incorporation of bullet-resisting protected positions that provide protection against the DBT

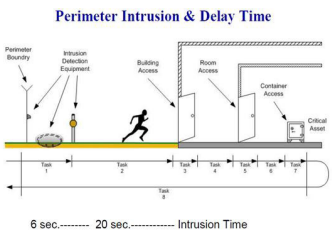
of fuel cycle facilities and transport of certain nuclear material. Under the program, security experts (primarily from NRC Headquarters and the NRC Region II office in Atlanta) carry out security inspections at fuel cycle facilities. The experts provide firsthand, independent assessments of site conditions and performance and document their findings in writing. They also conduct follow-up inspections to make sure the licensee has made any necessary corrections.

NRC Resident inspectors, in conjunction with NRC inspectors from Headquarters and the Region, monitor licensees' security-related activities on a daily basis. Security core inspections may include the following areas:

- Access Authorization
- Access Control
- Contingency Response Force-on-Force
- Equipment Performance, Testing, and Maintenance
- Protective Strategy Evaluation
- Protection of Classified and Safeguards Information
- Security Training
- Fitness-for-Duty Program
- Materials Control and Accounting
- Target Area Review
- Transportation Security

An NRC inspector gathers information at an NRC facility

The NRC's overall evaluation of licensee performance considers the results of all security inspections. At any time, if a significant security issue is identified, the NRC requires the licensee to resolve the issue promptly. If necessary, the NRC can take enforcement action that includes civil penalties. Some information related to these inspections is available to the public on the NRC website. Some information is not publicly available to protect sensitive security information.



Force-on-Force Security Inspections

An essential part of the NRC oversight of the security at Category I fuel cycle facilities is the force-on-force security inspection. Force-on-force inspections assess the ability of the licensee to defend the facility against the DBT for theft or diversion. The inspections also provide valuable insights that allow the NRC to evaluate and improve the effectiveness of the security programs at the facilities. The fuel cycle facility force-on-force program uses the same processes and many of the same staff as the force-on-force inspections performed at nuclear reactors.

As with nuclear power reactor programs, a full force-on-force inspection spans several weeks. It includes both tabletop drills and simulated combat between a mock adversary force and the security force at the facility. During the inspection, the mock adversary force attempts to reach Target Areas while battling the site's security force. Target Areas require protection from theft or diversion, and they must be protected from the adversary force.

Along with the facility's security personnel, many offsite organizations may participate in and observe force-on-force inspections, including Federal, State, and local law enforcement agencies. In addition, emergency planning officials, site operators, and NRC personnel are present.

Two members of the adversary force simulate a breach of the Protected Area at a site during a training exercise

By law, the NRC conducts a force-on-force inspection at Category I fuel cycle facilities 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 programs. The NRC is implementing changes to these force-on-force inspections, based on a lessons-learned review approved by the Commission.

The force-on-force program is as realistic as possible while also ensuring the safety of the employees and the public. The force-on-force inspection involves two sets of the security officers at the site. One set maintains site security and the other set participates in the inspection. In addition, a separate group controls and monitors both inspection participants and on-duty security officers during the inspection. The NRC has overall control of the exercise and the NRC inspection team monitors all aspects of the exercise activities to ensure

In force-on-force inspections, the use of weapons and explosives can be simulated using electronic equipment

the safety of the participants. The NRC also makes sure the exercise is conducted according to inspection standards. In preparation for a force-on-force inspection, NRC inspectors compile information from tabletop drills, facility tours, and security plan reviews. This information is then used to design a number of mock attacks seeking to probe for potential deficiencies in the site's defensive strategy. Any potentially significant findings identified during a force-on-force inspection are promptly reviewed, addressed, and corrected before the NRC inspectors leave.

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 mock adversary force, and assisting the NRC inspectors in evaluating site security forces and systems. It is important to emphasize that the NRC designs, runs, and evaluates the force-on-force inspections. The mock adversary force does not establish the inspection objectives, boundaries, or timelines.

CYBER SECURITY

Establishing and maintaining effective cyber security is a growing challenge across the Nation. New domestic and international adversaries continually emerge, as do new tools that can exploit potentially vulnerable systems and supply chains. Historically, digital computer systems played a limited role in the operation of nuclear facilities; however, digital systems are increasingly used to maximize plant productivity. Computer systems at operating reactors that monitor and control safety systems and help the reactor operate are isolated from external communications. Security systems that provide safeguards of the facility are also isolated from external communications, including the Internet. The NRC is working with its Federal partners to address the complicated issue of cyber security.

Established by the NRC in 2013 to strengthen internal governance of the agency's regulatory activities, the Cyber Security Directorate (CSD) plans, coordinates, and manages agency activities related to cyber security for NRC applicants and licensees. The CSD is responsible for rulemaking, guidance, licensing, policy issues, and oversight. Within the CSD is a cyber assessment team that assesses real world cyber events at NRC-licensed facilities. The team evaluates whether an identified threat could impact licensed facilities and makes recommendations for NRC actions and communications to the licensees. Additionally, the NRC participates with other Federal regulators and Executive branch agencies on the Cyber Security Forum for Independent and Executive Branch Regulators. Established in 2014, the forum brings together regulators to share best practices and lessons learned in cyber security protection for critical infrastructure. The NRC's Chairman serves as chair of the forum.

Following September 11, 2001, the NRC issued a series of advisories and orders requiring nuclear facilities to take certain actions, including enhancing the protection of their computer systems. Since that time, the NRC has replaced those interim measures with comprehensive regulations and added a cyber security threat component to both radiological sabotage and theft or diversion DBTs. Systems covered by the regulations include those related to safety, important to safety, security, and emergency preparedness functions. The regulations also cover support systems and equipment that,

if compromised, could impact safety, important to safety, security, and emergency preparedness functions. The NRC also published regulatory guidance for cyber security that provides an acceptable approach for protecting digital computers, communications systems, and networks from a cyber attack. All operating power reactor licensees have developed cyber security plans that the NRC has reviewed and approved. The NRC conducts inspections to ensure that operating power reactor licensees are implementing the cyber security requirements. In order to focus licensee cyber security resources on the most important digital assets, the NRC developed a consequence-based approach that provides for a graded application of cyber security controls. This reduces the regulatory burden while maintaining adequate protection. Ongoing high-profile cyber attacks on critical infrastructure underscore the importance of evaluating cyber security requirements for all classes of NRC licensees. The experience with operating power reactors has helped the agency develop new requirements promptly and effectively. In 2012, the NRC developed and issued a cyber security paper that communicated the staff's approach, or roadmap, to evaluating the need for cyber security requirements for fuel cycle facilities, nuclear power reactors, ISFSIs, and byproduct materials licensees. Implementing the roadmap will ensure that appropriate levels of cyber security actions are done in a timely and efficient manner at all NRC-licensed facilities and will identify whether any program improvements are needed.

The CSD is in the final stages of establishing new cyber security event notification requirements that will contribute to the NRC's analysis of the reliability and effectiveness of licensees' cyber security programs. These requirements will play an important role in the NRC's effort to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks.

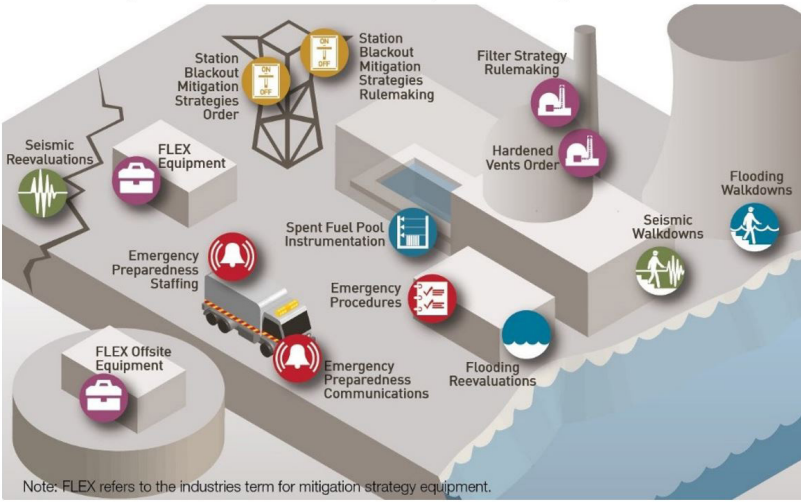
NUCLEAR PREPAREDNESS AND RESPONSE

Emergency Preparedness

For over 40 years, the NRC has provided regulatory oversight for emergency planning and incident response for its licensees. The licensee of each nuclear power reactor site must conduct a full scale exercise involving Federal, State, Tribal, and local agencies at least once every 2 years. The NRC and the Federal Emergency Management Agency (FEMA) evaluate these exercises to make sure that emergency preparedness programs and the skills of the emergency responders remain effective. The two agencies also identify and require corrections for any weaknesses. The NRC assesses the onsite response, while FEMA assesses the offsite response. In the years between evaluated exercises, licensees hold various drills to test key functions and maintain emergency responder skills.

Before 2001, few full-scale emergency preparedness exercises simulated hostile actions[4] against an operating reactor. After September 11, 2001, the NRC staff concluded that the emergency preparedness planning basis for operating reactors remained valid, even in the event of a hostile action incident. The emergency planning basis considers a wide range of accidents with established time frames and radiological characteristics. It looks at the impact upon a generic distance out to which predetermined

NRC Safety Enhancements for Beyond Design Basis Events



[4] Emergency preparedness exercises that simulate hostile actions against a nuclear power reactor are different from force-on-force security inspections, as discussed in the nuclear reactor security force-on-force section.

actions would provide dose savings to members of the public for any such accidents. It determines if pre-established actions would minimize a possible dose to members of the public for any such accidents. Studies have shown that the timing and magnitude of a release related to a hostile action event would be no more severe than the shortest duration or largest magnitude events considered in the emergency preparedness planning basis. However, a hostile action event presents new and unique challenges to emergency preparedness programs such as the coordination of law enforcement and emergency management personnel.

With that in mind, the NRC revised its regulations. Each site is now required to conduct an evaluated hostile action-based (HAB) exercise during every 8-year exercise cycle.

The NRC requires each nuclear power reactor licensee to:

- identify alternate emergency response facilities located offsite to support the mobilizing and staging of licensee emergency response staff
- promptly notify the NRC of potential or actual hostile actions against the nuclear power reactor site
- develop specific HAB emergency action levels for the classification of emergencies
- establish protective action strategies for onsite personnel in the event of a hostile action against the nuclear power reactor site

These measures are tested through drills and exercises, and are continually verified by NRC inspectors.

Incident Response

The NRC responds to incidents associated with all licensed facilities and activities. In addition, 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, consistent with the National Response Framework (NRF), and through Federal Interagency Operational Plans (FIOPs).

The members of the Executive Team discuss possible response measures during an Emergency Preparedness exercise

Headquarters Operations Center/Regional Incident Response Center(s)

The NRC directs its response to events from the HOC. The operations center is staffed 24 hours a day, 7 days a week, with two Headquarters Operations Officers. These officers have the experience and knowledge to evaluate and respond properly to reported events. Their actions may include: informing NRC management; informing the agency's Federal partners, licensees, and the media; and potentially staffing the HOC and/or one of the regional IRCs based on the direction of senior management. Recently, the HOC was upgraded to a new facility with advanced technology and improved equipment to enhance the NRC's ability to respond to events, including circumstances involving multiple facilities. The NRC's response capability also is improved through the continual training of responders, training and qualification of new staff, and reviews of response policies, processes, and procedures.

Each of the NRC's four regional IRCs has also been recently upgraded with advanced technology and equipment to enhance response to events. These upgrades allow for a seamless transition of response duties in the event that any of the other response centers become unavailable.

Interagency Response

The NRC coordinates its activities with other Federal agencies to improve its response to both nuclear safety and security emergencies. Using the NRF and FIOPs, the NRC works with Federal, State, Tribal, and local agencies in the prevention of, response to, and recovery from a nuclear safety or a hostile action event. The NRC has regularly provided 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, provides a framework for coordination and

Staff at the NRC's Headquarters Operations Center monitor simulated plant conditions during an Emergency Preparedness exercise with a nuclear power plant

information sharing among Federal agencies, State and local governments, and private sector critical infrastructure. The NIPP framework establishes roles and responsibilities of Federal, State, Tribal, local, and private sector critical infrastructure partners. Furthermore, the NIPP sets national priorities and goals for the effective distribution of funding and resources to enhance the resilience of the U.S. Government, economy, and public services in the event of natural or man-made disasters.

The NRC actively supports FEMA's National Exercise Program. This program is the principal mechanism for examining the preparedness, and measuring the readiness, of the United States to perform missions or functions that prevent, protect against, respond to, recover from, and mitigate all hazards. Scenarios are developed that potentially involve simulated weapons of mass destruction, major storms, or terrorist attacks. These scenarios are designed to test the Nation's ability to respond and recover from such events. Participating in these exercises provides the NRC with feedback to enhance its response program.

Integrated Response Program

The Integrated Response Program is designed to improve the effectiveness of law enforcement tactical team responses to a licensee's request for help to address a threat or attack. The program addresses beyond Design Basis Threats for which the government has the primary response function. The Integrated Response Program emphasizes communication and coordination between law enforcement and key personnel at the nuclear power reactor. It also facilitates a seamless interface of private and government tactical response assets in protecting the Nation and its infrastructure. In collaboration with DHS, the Federal Bureau of Investigations (FBI), and the power reactor industry, this program focuses on clearly identifying resources, roles, and responsibilities of the response organizations. The program also facilitated development of a computer-based navigational and response planning tool for the tactical response team. The partners are working towards exercising these response plans and the computer tools to continue enhancing tactical training and response capability.

Continuity of Operations

Continuity of Operations (COOP) is a federally mandated requirement for all Federal agencies. The NRC's COOP Plan ensures that the agency can continue to perform time sensitive, vital functions that protect public health and safety. The plan also ensures the agency can support the overall Federal Government's National Essential Functions following a major event that disrupts normal operations.

To be able to meet changing requirements and provide an effective response during a major event

The Team Approach

Effective preparedness and response requires cooperation among the Federal Government, State, and local officials, the public, and the NRC licensees

affecting NRC facilities, the NRC's COOP plan is regularly reviewed and tested. It is also updated based on lessons learned from real-world events and exercises. The NRC recently conducted a significant upgrade of its COOP Plan and capabilities. Additions to this plan include such items as updated rosters, checklists of action items, relocation guidance, and greater detail on internal and interagency communications.

The NRC also periodically tests these procedures, and at a minimum, participates in the annually-required national-level COOP exercise series. During these exercises, the NRC transfers functions to alternate locations, practices COOP procedures, and conducts internal and interagency communication tests. This demonstrates NRC's ability to meet Federal COOP and NRC mission requirements during even the most trying of events. Due to NRC's recent COOP revisions, the NRC's COOP program has gained interagency recognition, including high marks from interagency external evaluators during a recent national-level exercise.

ADDITIONAL SECURITY ACTIVITIES

Communications

An important part of protecting nuclear facilities from acts of terrorism is effective communication between the NRC, NRC-licensed facilities and certificate holders, and Federal, State, Tribal, Territorial, and local governments. The NRC continues to enhance its communications with new technologies and upgrades. One recent update includes installing a protected web-based computer server system to exchange sensitive security information quickly with licensees and authorized government officials. Using secure transmission equipment, the NRC can rapidly communicate classified and sensitive unclassified voice, data, and video information among NRC Headquarters, NRC Regional offices, and licensees.

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

- U.S. Department of Defense
- U.S. Department of Energy (DOE)
- DOE National Nuclear Security Administration
- U.S. Department of Homeland Security (DHS)

NRC staff speak at the Regulatory Information Conference in March of 2015

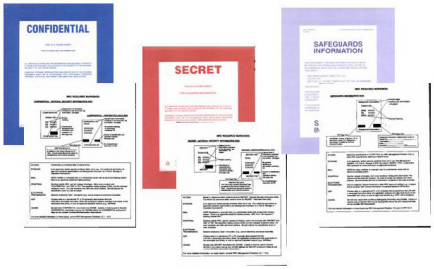
- DHS Federal Emergency Management Agency (FEMA)
- DHS Transportation Security Administration
- DHS Domestic Nuclear Detection Office
- U.S. Department of State
- U.S. Department of Transportation (DOT)
- Federal Aviation Administration
- Federal Bureau of Investigation (FBI)
- National Security Council
- North American Aerospace Defense Command (NORAD)
- U.S. Northern Command
- Office of the Director of National Intelligence
- National Counterterrorism Center
- Other members of the Intelligence Community

In addition, the NRC communicates directly with other Federal agencies about specific threats. For example, NORAD contacts the NRC directly to share information about potential aircraft threats against NRC regulated nuclear facilities. This communication and coordination lays the foundation for ongoing national efforts to detect, prevent, and respond to terrorist attacks.

The NRC continues to explore ways to share information that will make the Nation better informed and prepared while preventing unauthorized individuals from gaining access to sensitive information that might compromise security at NRC regulated facilities. The NRC must always balance its commitment to openness with the need to prevent the release of sensitive information.

Information Security

The NRC's information security program protects classified Restricted Data (RD) and National Security Information (NSI), SGI, and other sensitive information (e.g. sensitive unclassified nonsafeguards information (SUNSI)) from unauthorized disclosure. Only those with the requisite security clearance and/or a need-to-know, as applicable, can view such information. The NRC requires security clearances for appropriate individuals at NRC regulated facilities. These clearances enable licensee personnel to have access to sensitive information on a need-to-know basis. The NRC, in coordination with DOE, has developed comprehensive classification guides to protect sensitive nuclear technologies. This ensures that guidance on how to classify different types of information is applied consistently and is well understood.



The NRC has a long history of promoting openness and transparency in its regulatory and decision-making processes. The NRC is also dedicated to appropriately sharing information among organizations and licensees to enhance prevention and response to terrorist and other security incidents. In addition, the NRC remains diligent in controlling sensitive information to prevent unauthorized access by terrorists or other adversaries. The NRC continues to work to balance its commitment to openness with the public with the need to prevent unauthorized releases of sensitive information.

Intelligence

The NRC's intelligence staff assesses threats by reviewing and analyzing intelligence information and routinely communicating with intelligence and law enforcement agencies. 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 coordinator with other organizations and Federal agencies. The NRC ensures that its licensees, Agreement States, and Federal, State, and local authorities are promptly notified of any imminent threat or security incident. In addition, the staff annually reviews and briefs the Commission on the threat environment and any recommended changes to the DBTs.

The central mission of the NRC's intelligence staff is to evaluate and warn of possible threats against NRC or Agreement State licensees. Since the 1970s, the NRC has assessed a variety of threats to licensed nuclear facilities and radioactive materials. These threat assessments provide indications and warnings of potential attacks or other malevolent activities directed at nuclear facilities or radioactive material licensees. The intelligence staff assesses threats by reviewing thousands of classified and unclassified messages, evaluating intelligence products, and 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 threat's credibility and, working with NRC physical security counterparts, recommends protective actions to licensees. The NRC's intelligence staff also has a duty officer on call 24 hours a day, 7 days a week, to respond to security events and suspicious incidents at NRC-licensed facilities.

To assess and rapidly share critical, time-sensitive threat information, the NRC developed the Information Assessment Team (IAT) process. If the NRC receives information about a possible threat to one or more licensee sites, an Information Assessment Team Advisory (IATA) or a Security Advisory (SA) may be issued. An IATA communicates general security threat information. An SA is more specific to the operational impact of threat-related information. Both an IATA and an SA are non-public communications.

An IATA is issued to specific licensees within hours or less of receiving threat-related information on the following:

- changes to the Homeland Security Advisory System (HSAS) level
- when the FBI issues a Domestic Threat Advisory
- when a significant act of domestic terrorism or other malevolent act has occurred
- when the NRC becomes aware of intelligence information regarding statements or actions taken by foreign persons or by terrorist organizations, or other threat-related information, relating to NRC-licensed facilities or activities

An SA is issued to licensees regarding operational information directly related to the security and common defense of national infrastructure under NRC's authority. An SA requests each affected licensee to review the information for applicability to its facility or operations and consider actions, as appropriate, to avoid similar problems. An SA may be issued within days or less of receiving threat-related information on:

- an urgent security vulnerability that may affect a whole class or several classes of licensees
- additional information following notification via an IATA that the HSAS threat level has been raised
- National special security events
- recommended voluntary compensatory measures and actions for urgent security-related issues

Additional interactions involving the intelligence community, DOE, and the International Atomic Energy Agency (IAEA), among others, are conducted in order to keep up to date on the latest significant changes to safety and security information. Based on these interactions and information assessments, the NRC informs licensees of changes to the safety environment and threat landscape and interacts with its licensed facilities to improve safety and security accordingly.

Security Programs to Ensure Trustworthiness and Reliability

Access Authorization Programs

The NRC requires licensees to control who has access to their facilities. Before new employees or contractors are allowed to be unescorted in areas containing nuclear and radiological materials, they must pass several evaluations and background checks. These serve to determine if they are trustworthy and reliable individuals. The evaluations include verification

of identity, drug and alcohol testing, psychological evaluation, employment history, verification of education, credit history check, and criminal history check through the FBI.

Many licensees use biometrics as part of their access requirements

The NRC continually monitors the elements of the access authorization programs through inspections. The access authorization requirements employ a graded approach and may include the following depending on the type of facility:

- psychological assessments by licensed psychologists
- information sharing database used by licensees
- continuous behavioral observation
- a minimum 5-year reinvestigation of criminal and credit history records for all individuals with unescorted access
- self-reporting of legal actions by individuals with unescorted access
- a 5-year psychological reassessment and a 3-year background reinvestigation for certain critical job functions, such as individuals who have an electronic (cyber) means to adversely impact facility safety, security, or emergency preparedness

Fitness-for-Duty Program

The NRC requires licensees of operating reactors, new reactors, and fuel cycle facilities to have a fitness-for-duty program. The cornerstone of these programs is drug and alcohol testing and behavioral observation. The fitness-for-duty program provides reasonable assurance that nuclear facility personnel are trustworthy, reliable, not under the influence of any substance (legal or illegal) or mentally or physically impaired. Individuals are subject to drug and alcohol testing prior to gaining unescorted access (i.e., pre-access testing) and at random throughout the year. At least half of the number of individuals in the testing program are to be tested annually. Testing will also occur if circumstances warrant additional attention, such as when an individual

NRC requires drug and alcohol testing of personnel who perform safety-sensitive and security-sensitive work at nuclear power plants and Category I fuel cycle facilities

exhibits signs of possible impairment, after an accident, or to ensure that an individual who previously tested positive continues to maintain abstinence. NRC regulations include detailed procedures on the collection of specimens, laboratory testing, and medical review of test results. This ensures the integrity of the testing process and affords due process to tested individuals.

Drug testing equipment at a Licensee Testing Facility

Since 2009, NRC regulations also require licensees to manage the work hours of certain workers at operating reactors and to mitigate the potential for chronic and cumulative fatigue by following work-hour limits. Licensees also are required to conduct and document a fatigue assessment if, among other things, an individual conducting certain duties reports that they are unfit for work because of fatigue. Licensees must also do an assessment if a worker is seen to be inattentive. As part of the fatigue management process, a licensee must implement procedures to ensure that any person who self-reports they are fatigued will not be retaliated against for that disclosure.

Behavioral Observation Program

The NRC requires certain nuclear facilities to implement a behavioral observation program. This program is conducted by all personnel within a facility who are trained specifically on behavioral observation techniques. The program looks for individual behavioral changes that could indicate a person might act in a manner detrimental to public safety if unmonitored or left unaddressed. Employees are offered counseling if they have job performance problems or exhibit unusual behavior. Similarly, employees who appear to be under the influence of drugs or alcohol are immediately removed from the work area for evaluation under the licensee's fitness-for-duty program.

Insider Mitigation Program

The insider mitigation program contains elements of the access authorization, fitness-for-duty, cyber security, and physical protection programs at certain nuclear facilities. The insider mitigation program helps ensure that those who are allowed to be in protected areas within a nuclear facility without an escort 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 nuclear facility to cause damage or sabotage or potentially aid

an adversary. This program is essential to the overall security of certain nuclear facilities.

NRC requires fingerprinting for persons with unescorted access to sensitive areas of facilities and information

International Safety and Security

The NRC's international activities are wide-ranging. They include treaty implementation, nuclear non-proliferation, export-import licensing for nuclear materials and equipment, international safeguards support and assistance, international safety and security cooperation and assistance, and international safety and security information exchange. These activities support the NRC's domestic mission as well as broader U.S. domestic and international interests.

Congress made the NRC the export-import licensing agent for the U.S. Government for nuclear materials and equipment. For exports, the NRC regulations in 10 CFR Part 110, "Export and Import of Nuclear Equipment and Material," state that security measures in countries receiving nuclear material must provide protection at least to the same level as the recommendations in the IAEA publication INFCIRC/225, "The Physical Protection of Nuclear Material and Nuclear Facilities." On January 1, 2015, the NRC adopted Revision 5 of the document as its physical protection licensing criterion for the export of nuclear materials.

In 2004, the U.S. Government made a commitment to implement the IAEA Code of Conduct for the Safety and Security of Radioactive Sources (the Code) and its associated Guidance on Import and Export of Radioactive Sources (the Guidance). The U.S. commitment to the Code became binding law in the Energy Policy Act of 2005. The NRC considered the provisions of the Code and Guidance in its domestic regulations governing use, transfer, and tracking of 16 radionuclides. Strong international support for the Code and the Guidance is shown by the 115 countries that have agreed to implement the Code and 79 that have agreed to implement the Guidance (as of January 2015). The NRC continues to support the development and implementation of the Code and its associated Guidance.

The NRC participates in the annual General International Conference for the International Atomic Energy Agency (IAEA) in Vienna, Austria

In 2005 and 2010, the NRC implemented rules with enhanced controls over the import and export of radioactive sources. Under the amendments, licensees must apply for specific licenses to export certain radioactive sources listed in 10 CFR Part 110, Appendix P, "Category 1 and 2 Radioactive Material." This includes the radioactive sources contained in the Code. Licensees are also required to document that the end user is authorized to receive and possess the material and must provide advance notice of shipments. For the export of these sources, the NRC makes an assessment and determines whether the importing country's regulatory infrastructure is sufficient to maintain adequate control over the material. In countries without adequate regulatory controls, the Code provides for "exceptional circumstances" under which high risk sources can be exported with additional conditions imposed on the licensee.

The NRC has maintained extensive engagement with international organizations such as the IAEA. The NRC, in partnership with other U.S. agencies, works to strengthen the international physical protection framework. This is done by providing technical expert support to the IAEA and by supporting U.S. policy initiatives worldwide. The NRC helps to develop international security guides and recommendations. This participation allows the NRC to share its experience broadly with the international community and learn from others' experiences. In 2013, as part of the U.S. commitment made during the 2010 Nuclear Security Summit in Washington, DC, the NRC received an IAEA International Physical Protection Advisory Service (IPPAS) mission. IPPAS missions provide peer advice on implementing international and IAEA guidance on the protection of nuclear and other radioactive material and associated facilities. The IPPAS team concluded that nuclear security within the U.S. civilian nuclear sector is robust and sustainable.

To support the exchange of best security practices, NRC staff participates in U.S. interagency bilateral physical protection visits to foreign countries possessing or expecting to receive U.S. nuclear material. The NRC also participates in the U.S. Government interagency process to maintain and expand the framework of bilateral and multilateral peaceful nuclear cooperation agreements. These provide a basis for nuclear cooperation with other countries, including transfers of

nuclear materials, equipment, and technology.

To promote international cooperation, the NRC hosts meetings and tours to demonstrate U.S. physical protection practices. The NRC also provides training and technical support to foreign partners. For example, in 2012, the NRC hosted an International Regulators Conference on Nuclear Security. It was the first major meeting for regulatory agencies from many countries to discuss radioactive material and nuclear security oversight issues. The conference focused on the importance of comprehensive national regulatory security programs. It also promoted building relationships with other regulatory entities responsible for security at civilian nuclear facilities. Furthermore, the NRC provides international assistance to foreign regulatory counterparts for improving safety and security of civilian uses of radioactive materials; fosters international technical cooperation, sharing regulatory and operational experience; and demonstrates leadership on regulatory issues, both within the international community and the U.S. Government.

CONCLUSION

Protecting the Nation's civilian nuclear facilities and the use of radioactive materials is a top priority of the NRC. The NRC works aggressively to protect the public health and safety, promote the common defense and security, and protect the environment by regulating the commercial nuclear industry. Working closely with its partners, the NRC will continue to remain vigilant and provide oversight of security and emergency preparedness activities at licensed nuclear facilities.

NRC Chairman Stephen G. Burns and his Commission colleagues speak to members of the Senate Energy and Water Appropriations Subcommitee. From left to right: Commissioner Jeff Baran, Commissioner Kristine L. Svinicki, Chairman Stephen G. Burns, and Commissioner William C. Ostendorff

GLOSSARY

Agreement State

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

Applicant

A person or an entity applying for a license, permit, or other form of Commission permission or approval under 10 CFR Parts 30, 40, 50, 52, 61, 70, or 72.

Category I Fuel Cycle Facilities

Fuel cycle facilities that possess more than 5,000 grams (about 11 pounds) of strategic special nuclear material (defined as a "formula quantity") or more as computed by the formula, grams = (grams contained U-235) + 2.5 (grams U-233 + grams plutonium).

Classified Information

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

1. National Security Information (NSI): Information classified by an Executive Order, whose compromise would cause some degree of damage to national security.
2. Restricted Data (RD): Information classified by the Atomic Energy Act of 1954, as amended, whose compromise would assist in the design, manufacture, or use of nuclear weapons.

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

Depleted Uranium

Source material uranium in which the isotope uranium-235 is less than 0.711 weight percent of the total uranium present. Depleted uranium does not include special nuclear material.

Design Basis Threat

A profile of the type, composition, and capabilities of a possible adversary. The NRC, and certain licensees and applicants under 10 CFR Parts 50 and 52, use the DBT as a basis for designing safeguards systems to protect against acts of

radiological sabotage and to prevent the theft or diversion of special nuclear material. The DBT clearly identifies 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 decision-making during emergencies. The emergency preparedness process incorporates the means to rapidly identify, evaluate, categorize, and react to a wide spectrum of emergency conditions.

Federal Interagency Operational Plans

FIOPs, one for each preparedness mission area (Prevention, Protection, Mitigation, Response, and Recovery), describe how the Federal Government aligns resources and delivers core capabilities.

Hostile Action

An act toward a nuclear power plant or radioactive material facility or its personnel that includes the use of force to destroy equipment, take hostages, or intimidate the licensee to achieve an end. This covers 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 incorporated.

Integrated Response

A program designed to assess and integrate law enforcement tactical response capabilities on a nuclear power plant site-specific basis. The effort combines Federal, State and local law enforcement, complemented by site security personnel deploying a defense-in-depth strategy.

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 authorized by the NRC to conduct the following activities:

- constructing, operating, and decommissioning commercial reactors and fuel cycle facilities
- possessing, using, processing, exporting, importing, and certain aspects of transporting nuclear materials and waste
- siting, designing, constructing, operating, and closing waste disposal sites

Nonpower Reactor

Nuclear reactors primarily used for research, training, and development. Formerly referred to as research and test reactors.

NRC Headquarters Operations Center

The NRC HOC is located in Rockville, MD, and 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 HOC 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 Reactor

An electrical generating facility that uses a nuclear reactor as its heat source to provide steam to a turbine generator. Also referred to in this document as an operating reactor.

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 IAEA, "safeguards" refers to verification that the "peaceful use" commitments made in binding nonproliferation agreements, both bilateral and multilateral, are honored.

Safeguards Information (SGI)

A special category of sensitive unclassified information authorized to be protected under Section 147 of the Atomic Energy Act of 1954, as amended. SGI concerns the physical protection of operating 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 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 Nonsafeguards Information (SUNSI)

SUNSI is generally not publicly available and encompasses a wide variety of categories (e.g., personally identifiable information protected under the Privacy Act of 1974, attorney-client privilege, investigations information, confidential and sensitive allegations, confidential source, official use only-security related information).

Under 10 CFR 2.390, "Public Inspections, Exemptions, Requests for Withholding," information about a licensee's or applicant's physical protection or material control and accounting program for special nuclear material not otherwise designated as SGI or classified as National Security Information or Restricted Data must be protected in the same manner as commercial or financial information. In other words, such information is exempt from public disclosure. Policy and procedures related to sensitive unclassified non-safeguards information are the responsibility of the NRC Office of Information Services.

Special Nuclear Material

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

Spent Fuel Pool

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

Spent Nuclear Fuel

Fuel that has been withdrawn from a nuclear reactor following irradiation, has undergone at least 1 year's decay since being used as a source of energy in a power reactor, and has not been chemically separated into its constituent elements by reprocessing. Spent fuel includes the special nuclear material, byproduct material, source material, and other radioactive materials associated with fuel assemblies.

LIST OF ACRONYMS

CFR	Code of Federal Regulations
COOP	Continuity of Operations
CSD	Cyber Security Directorate
DBT	Design Basis Threat
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
FBI	Federal Bureau of Investigations
FEMA	Federal Emergency Management Agency
FIOP	Federal Interagency Operational Plan
HAB	Hostile Action-Based
HOC	Headquarters Operations Center
HSAS	Homeland Security Advisory System
IRC	Incident Response Center
IAEA	International Atomic Energy Agency
IAT	Information Assessment Team
IATA	Information Assessment Team Advisory
IPPAS	International Physical Protection Advisory Service
ISFSI	Independent Spent Fuel Storage Installation
LVS	License Verification System
NIPP	National Infrastructure Protection Plan
NORAD	North American Aerospace Defense Command
NPR	Nonpower Reactor
NRC	U.S. Nuclear Regulatory Commission
NRF	National Response Framework
NSI	National Security Information
NSTS	National Source Tracking System

RD	Restricted Data
SA	Security Advisory
SGI	Safeguards Information
SUNSI	Sensitive Unclassified Nonsafeguards Information
WBL	Web-Based Licensing

NUREG/BR-0314, Rev. 4

August 2015