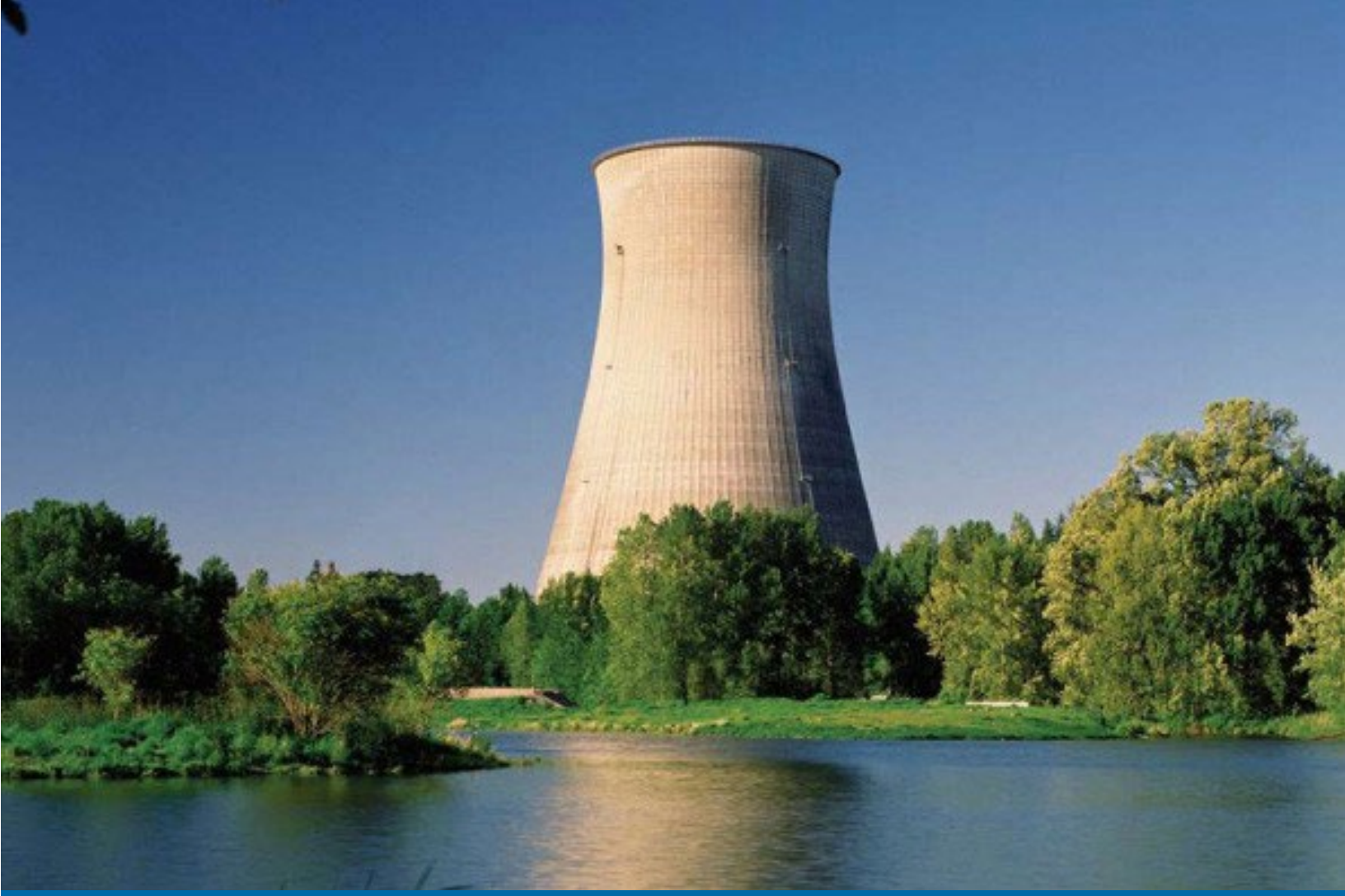


Nuclear Reactors, Materials, and Waste Sector-Specific Plan

An Annex to the NIPP 2013

2015

Homeland Security

TABLE OF CONTENTS

COORDINATION LETTER FROM COUNCIL CHAIRS

In 2003, the Secretary of Homeland Security established the Nuclear Reactors, Materials, and Waste Sector (or Nuclear Sector) as a critical infrastructure sector, recognizing the significant economic, environmental, and social contributions of its assets and resources. Since that time, the sector has successfully built a public-private partnership that works on a voluntary basis to improve information sharing, inform policy, reduce risks in the use of nuclear materials, and develop tools and exercises to improve security and resilience planning, response, and recovery. This Nuclear Sector-Specific Plan (SSP) is designed to continue guiding the sector's voluntary, collaborative efforts to improve security and resilience over the next four years.

2015 Sector-Specific Plan Update

This 2015 release of the Nuclear Sector-Specific Plan updates the original plan issued in 2010. As with the previous plan, this Sector-Specific Plan represents a collaborative effort among the private sector; State, local, tribal, and territorial governments; non-governmental organizations; and Federal departments and agencies to identify and work toward shared goals and priorities to reduce critical infrastructure risk.

The Nuclear Sector Coordinating Council and Government Coordinating Council jointly developed the Nuclear Sector goals, priorities, and activities in this SSP to reflect the overall strategic direction for the Nuclear Sector. The Sector's goals support the Joint National Priorities developed in 2014 by the national council structures described in the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience (NIPP 2013)*.

This Sector-Specific Plan also reflects the continued maturation of the Nuclear Sector partnership and the progress made since the 2010 SSP to address the evolving risk, operating, and policy environments.

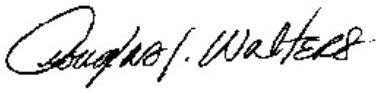
Key Accomplishments

Since 2010, Nuclear Sector partners in the public and private sectors have taken significant steps to reduce sector risk, improve coordination, and strengthen security and resilience capabilities:

- Planned and conducted **integrated response exercises** with the Federal Bureau of Investigation, the Nuclear Regulatory Commission, and private sector partners.
- Conducted a cross-sector **planning workshop** with the Food and Agriculture Sector focused on communication protocols for a major radiological contamination, which included representatives from seven Federal agencies and three States.
- Implemented a number of upgrades and changes to nuclear power plants following the 2011 Fukushima incident in Japan, including the establishment of **two emergency response centers** that can provide a full set of emergency equipment to any U.S. nuclear facility within 24 hours of an accident or incident.
- Implemented the computerized **National Source Tracking System** to track high-risk sources from when they are manufactured or imported to their disposal or export.
- Developed the ***Roadmap to Enhance Cyber Systems Security in the Nuclear Sector***, which provides a vision and framework for mitigating cybersecurity risks to the wide variety of systems critical to commercial nuclear power plant operations.

These achievements, which represent the effective collaboration of the Nuclear Sector Coordinating Council, Government Coordinating Council, and Sector-Specific Agency, clearly demonstrate the sector's progress in working toward a rational approach to develop, prioritize, and implement effective security programs and resilience strategies.

In the same shared purpose that guided these actions, Nuclear Sector partners look forward to continuing their efforts to enhance the security and resilience of our Nation's critical infrastructure assets.



Doug Walters
Chair
Nuclear Sector
Coordinating Council

Caitlin A. Durkovich
Assistant Secretary
DHS Office of Infrastructure Protection
Chair, Nuclear Government Coordinating Council

EXECUTIVE SUMMARY

Nuclear power reactors generate 20 percent of U.S. electricity, while more than 20,000 licensees use nuclear materials in diagnosis and and medical therapy—an estimated 20 million medical procedures each year in science and biomedical research—for irradiation of food and medical products, and during construction and oil exploration. Accidents, failures, or disruptions in the Nuclear Sector could have severe human health and safety consequences and cascading effects on critical infrastructure sectors that rely on nuclear power or nuclear medicine and industrial uses. Uniquely hazardous characteristics make Nuclear Sector assets the most highly regulated and heavily guarded of all civilian infrastructure.

Nuclear Sector Assets and Risks

The Nuclear Reactors, Materials, and Waste Sector (or Nuclear Sector) includes the Nation's 99 commercial nuclear power plants; 31 research, training, and test reactors (RTTRs); 8 active fuel cycle facilities; waste management; and 18 power reactors and 6 fuel cycle facilities that are decommissioning or inactive. It also includes the transport, storage, use, and safe disposal of more than 3 million packages of radioactive or nuclear materials and waste annually.

The Nuclear Sector's contributions to the Nation are countered by the magnitude of the potential consequences that could be associated with the failure, damage, or disruption of critical assets. The private sector primarily owns and operates all civilian nuclear assets under a large framework of regulations that require robust and redundant security measures and specialized emergency response. The design basis threat (DBT)—an assessment that identifies all adversaries and attack capabilities that threaten a specific site—defines the minimum security protections for high-risk facilities. Security is regularly tested and inspected through Force-on-Force exercises employing a mock adversary.

The Nuclear Sector mitigates against a well-defined profile of risks to nuclear material from accidents, attacks, and malevolent or inadvertent misuse. Yet several emerging issues have the potential to exacerbate sector risks. Climate change and increasingly severe natural disasters increase risks for nuclear power plants, many of which are operating with aging equipment. After a March 2011 earthquake and tsunami caused an unforeseen triple meltdown at Japan's Fukushima-Daiichi nuclear power plant, U.S. nuclear facilities are re-evaluating their ability to withstand beyond-design-basis events. Increasingly sophisticated cyber threats require continually advancing cybersecurity requirements for critical plant control systems.

The Nuclear Sector also heavily relies on a limited and highly international supply chain—the United States imports more than 90 percent of its domestically consumed isotopes. A rapidly shrinking number of international medical isotope suppliers could create significant shortages in the medical community.

Partnering to Improve Security and Resilience

The Nuclear Regulatory Commission (NRC) regulates the civilian use of nuclear material using a robust framework that requires all licensees to meet extensive safety and security requirements. The majority of the sector's risk management activities are not voluntary. However, owners and operators have formed associations, working groups, and other mechanisms to share information, exchange best practices, and partner on security and resilience activities beyond what is required by regulation.

The *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013) partnership structure encourages owners and operators to work directly with their peers through the Sector Coordinating Council (SCC) and with Federal, State, local, tribal, and territorial partners through the Government Coordinating Council (GCC). Partners work on a voluntary basis to share actionable, relevant risk information; conduct voluntary site assessments and deploy facility security enhancements to reduce physical, human, and cyber risks; support research and development into new simulation and security technologies; and examine new technologies that reduce or eliminate the use of radioactive materials in medical and industrial applications.

2015 Sector-Specific Plan

This Nuclear Sector-Specific Plan (SSP) is designed to guide the sector's voluntary, collaborative efforts to improve security and resilience during the next four years. It describes how the Nuclear Sector manages risks and contributes to national critical infrastructure security and resilience, as set forth in Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21). As an annex to the NIPP 2013, this Sector-Specific Plan tailors the strategic guidance provided in the NIPP 2013 to the unique operating conditions and risk landscape of the Nuclear Sector. As such, the sector strategy

supports the NIPP 2013 national goals and strategy, the 2014 Joint National Priorities, and implementation of Executive Order 13636: Improving Critical Infrastructure Cybersecurity (EO 13636).

Sector Goals, Priorities, and Activities

As part of this 2015 Sector-Specific Plan, the Nuclear SCC and GCC have identified goals and priorities to guide the sector's voluntary security and resilience efforts over the next four years and to address or mitigate the sector's risks.

The councils set five overarching goals for Nuclear Sector security and resilience:

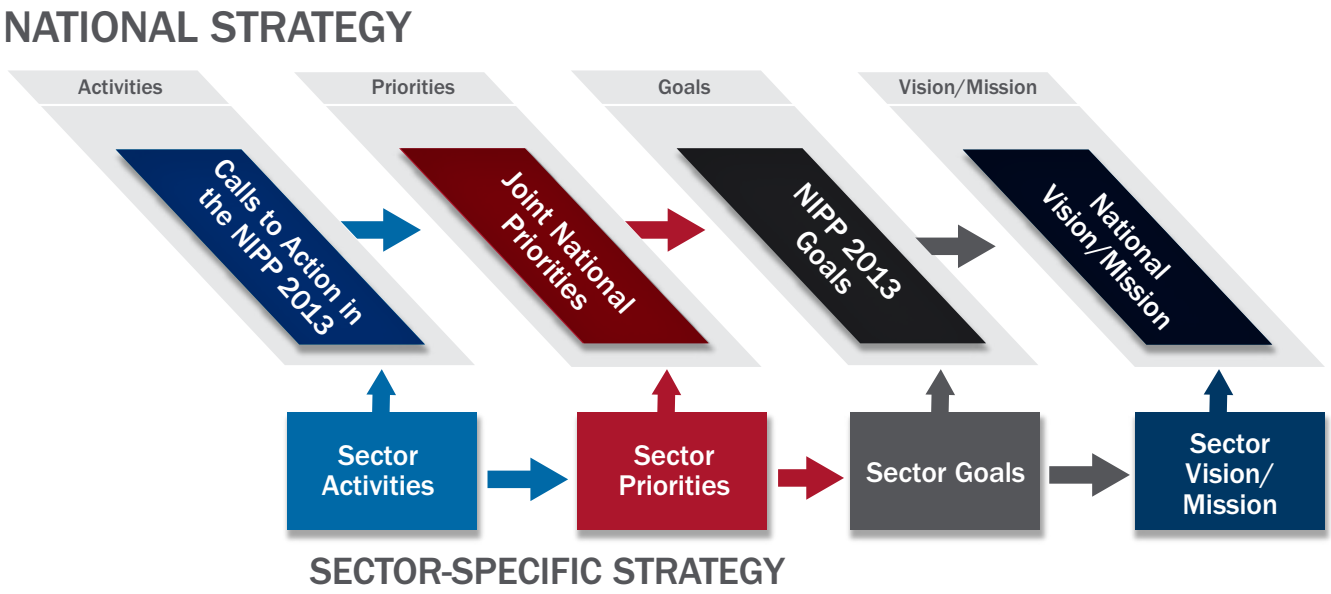
1. Establish robust collaboration and communication and promote continuous learning among Nuclear Sector partners and cross-sector stakeholders.
2. Continuously identify and assess sector-specific threats, vulnerabilities, and consequences to enable a risk-informed approach to security and resilience enhancements.
3. Coordinate with sector partners to develop programs and measures that cost-effectively reduce physical and cyber risks from all-hazard incidents impacting Nuclear Sector assets.
4. Support advance planning and risk mitigation that enables coordinated response and rapid recovery to ensure safe and resilient operation of critical Nuclear Sector services.
5. Promote continuous learning and adaptation among global Nuclear Sector and cross-sector partners during exercises, incidents, and planning.

To achieve these goals, sector partners developed nine priorities to focus their efforts:

- Promoting voluntary sector and cross-sector coordination and partnerships with the international community.
- Improving the delivery of relevant risk information and actionable alerts to sector partners.
- Increasing public awareness of sector security measures and responses.
- Identifying and characterizing evolving sector-specific physical, cyber, and human risks.
- Improving the security of sector cyber assets, systems, and networks.
- Improving the security, tracking, detection, and disposal of nuclear and radioactive material.
- Supporting permanent risk reduction by transitioning to non-isotopic or lower-activity radioactive source technologies.
- Increasing awareness and coordination with first responders at the State, local, tribal, and territorial levels.
- Promoting voluntary exercises with security and emergency response stakeholders to improve preparedness, response, and recovery.

As part of a detailed implementation plan, the sector identified 15 activities that sector partners plan to undertake. Chapter 4 provides a detailed list of these activities. While risk management in the Nuclear Sector is substantially regulated by the NRC, the Nuclear SSP activities presented here reflect only the voluntary activities that the Nuclear SCC and GCC will participate in or support to reduce risk beyond what is accomplished by regulation alone. The Nuclear SCC and GCC may pursue the following activities under either joint or individual council efforts over the next one to four years.

Figure ES-1: Alignment of National and Sector-Specific Goals, Priorities, and Activities



1 INTRODUCTION

This *Nuclear Reactors, Materials, and Waste Sector-Specific Plan* 2015 (SSP) sets the strategic direction for voluntary, collaborative efforts to improve sector security and resilience over the next four years. It describes how the Nuclear Reactors, Materials, and Waste Sector (or Nuclear Sector) manages risks and contributes to national critical infrastructure security and resilience, as set forth in Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21). As an annex to the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013), this SSP tailors the strategic guidance provided in the NIPP 2013 to the unique operating conditions and risk landscape of the Nuclear Sector. As such, this sector strategy supports the NIPP 2013 national goals and strategy, the 2014 Joint National Priorities, and implementation of Executive Order 13636: Improving Critical Infrastructure Cybersecurity (EO 13636).

This plan describes the Nuclear Sector's approach to risk management and national preparedness—considering its distinct assets, operations, and risk profile. In this 2015 SSP, public and private sector members of the Nuclear Sector Coordinating Council (SCC) and Government Coordinating Council (GCC) identified a shared vision, goals, and priorities for sector security and resilience and developed a supporting set of collaborative activities they plan to pursue during the next four years, as resources allow.

SSP development answers NIPP 2013 Call to Action #2, which requires each of the 16 designated critical infrastructure sectors to update their SSP every four years to reflect joint sector priorities, address sector reliance on lifeline functions, describe national preparedness efforts, outline cybersecurity efforts, and develop metrics to measure progress. Appendix B illustrates how the Nuclear Sector's priorities support both the NIPP 2013 national goals, the five Joint National Priorities, and the 12 Calls to Action in the NIPP 2013.

The remainder of this Nuclear SSP is organized as follows:

- **Chapter 2: Sector Overview**—Provides an overview of the sector's assets and operating characteristics, risk profile, and key public and private sector partners.
- **Chapter 3: Risk Management and National Preparedness**—Describes the mechanisms to achieve sector goals, including ongoing and planned partnership programs, activities, and resources that support the sector's current risk management approach; R&D priorities; and how the sector supports national preparedness through incident response and recovery.
- **Chapter 4: Vision, Goals, and Priorities**—Presents the sector's vision, updated goals, and priorities for Nuclear Sector security and resilience over the next four years, and the specific activities that the Nuclear Sector public and private sector stakeholders plan to conduct.
- **Chapter 5: Measuring Effectiveness**—Describes the planned approach to measure the effectiveness of individual activities and report on sector progress.

This SSP provides targets for collaborative planning among the U.S. Department of Homeland Security—which serves as the Sector-Specific Agency—and Nuclear Sector partners in the public and private sectors, represented by the Nuclear GCC and SCC. Partners have a clear and shared interest in ensuring the security and resilience of critical sector assets, and this plan represents the voluntary, collaborative activities that could greatly reduce sector risk and build resilience during the next four years.

2 SECTOR OVERVIEW

This chapter profiles the Nuclear Sector's assets, design, and operating characteristics; identifies its primary risks and interdependencies, and describes how the sector's public-private partnership operates.

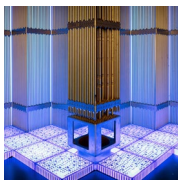
2.1 Sector Profile

The U.S. civilian Nuclear Sector includes the Nation's 99 commercial nuclear power plants at 61 sites; 31 non-power reactors used for research, training, and radioisotope production; fuel-cycle facilities; and nuclear and radioactive materials used in medical, industrial, and academic settings. Additional assets include power reactors and other nuclear facilities that are under construction, and those that are being decommissioned and dismantled. The sector also includes the transportation, storage, and disposal of nuclear materials, and radioactive waste. Sector assets range from large reactor sites to small, sealed sources that can be easily transported by a single individual.

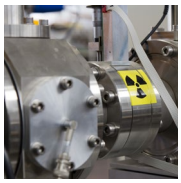
Nuclear Sector assets are generally owned and operated by the private sector, but are the most highly regulated and heavily guarded of all civilian infrastructure. Public access to the highest-hazard nuclear materials is tightly controlled. The Nuclear Regulatory Commission (NRC) regulates the civilian use of nuclear material using a robust framework that requires all licensees to meet safety and security requirements to ensure the protection of public health and safety, the environment, and national security. The NRC requirements are not voluntary. Owners and operators within the subsectors have formed associations, working groups, or other mechanisms to facilitate intelligence and risk information sharing and to exchange best practices for safety, security, and resilience beyond what is required by regulation.

This Sector Profile provides a snapshot of Nuclear Sector assets and key characteristics that influence security and resilience in the sector.

Key Sector Operating Characteristics



Nuclear power plants are among **the most physically hardened U.S. infrastructure**, using defense-in-depth security that employs independent, redundant layers of defense to guard against single-point failures. High-risk facilities are required to protect against the design basis threat (DBT)—an NRC assessment that defines all adversaries and attack capabilities that threaten the specific site. Security is regularly tested and inspected through exercises employing a mock adversary.



The sector depends on an **international and very limited supply chain of materials**. Some major components have only one supplier in the world, and overseas manufacturing of critical parts or radioactive materials introduces risk for counterfeiting and supply chain disruption.

Public **access to key facilities and assets is tightly controlled**. Tours, open houses, and other public events are highly orchestrated and areas open to visitors are restricted. Multiple security barriers, such as guard stations and armed security guards, fences, barriers, and alarms, are plainly visible.

High economic significance and public safety implications result in a **large national security interest** in Nuclear Sector facilities. Nuclear facilities vary in their **proximity to high-density population centers**. Most of the larger plants and facilities initially were built in remote areas; however, during decades of operation, development has encroached on individual plants, in many cases increasing the consequences of a site disruption.

The **highest concentration of nuclear power plants** is along the East Coast and Great Lakes area, with a smaller concentration of plants on the Gulf Coast and in the Midwest. There are a number of large nuclear power plants in Texas, Arizona, and California.

NUCLEAR SECTOR SNAPSHOT (2015)

KEY ASSETS

99
nuclear power reactors generate 20% of U.S. electricity

18
decommissioning power reactors

3 million
packages of radioactive material shipped yearly

8 active
fuel cycle facilities

31
operating research test reactors

>20,000
licensees of radioactive materials for medical, research, and industrial purposes

OWNERS AND OPERATORS

- 25 private companies and public power utilities own and operate all 99 U.S. nuclear power reactors at 61 sites.
- Universities own most of the 31 operating research test reactors; some are owned by private and Federal entities.
- More than 20,000 licenses are held by public and private organizations for medical, industrial, and academic uses of source, byproduct, and special nuclear materials.
- The Nuclear Sector does not include Department of Defense (DOD) or Department of Energy (DOE) defense-related nuclear facilities or nuclear materials.

REGULATION

- The independent **NRC regulates and licenses all civilian nuclear power plants and operations**, including reactors, radioactive materials, fuel cycle facilities, and materials transportation, storage, and disposal.
- NRC issues **policies, rules, and orders** that govern nuclear reactor and material safety and security—making it one of the most highly regulated U.S. infrastructure sectors.
- Under formal agreements with the NRC, **37 Agreement States assume regulatory responsibility** for approximately 18,000 materials licensees under State regulations that meet NRC standards.

PRIMARY SECTOR INTERDEPENDENCIES

Energy—Nuclear facilities both supply electricity and depend heavily on uninterrupted power for continuous safe operations.

Transportation Systems—Nuclear and radioactive materials are shipped worldwide via air, rail, highway, and water.

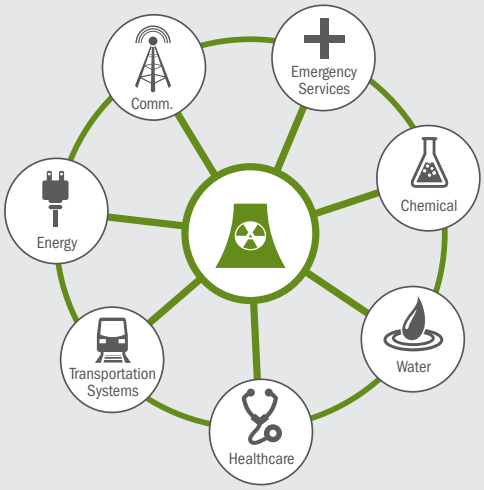
Communication—Communication is critical to normal and emergency operations, both onsite and with critical partners.

Healthcare—North America performs about 20 million medical procedures each year using radioactive materials.

Chemical—Chemicals are used daily in the production of electricity.

Water—Nuclear power plants use large quantities of water for cooling. Interrupted water supply may require shut down.

Emergency Services—The Nuclear Sector's uniquely hazardous characteristics require trained emergency responders during any incident.



Subsector Assets and Operations

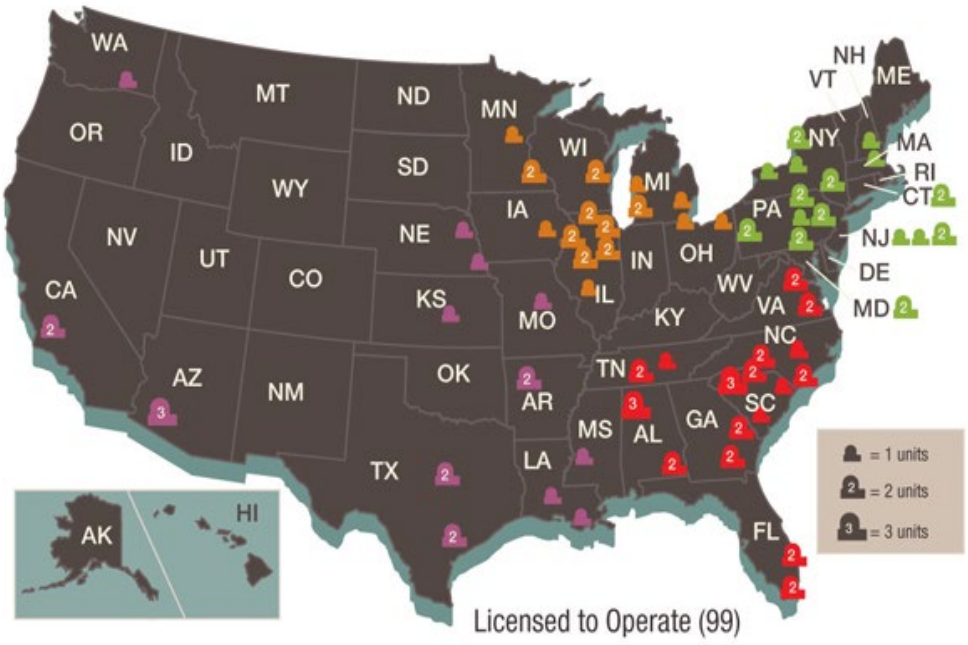
Nuclear Power Plants with Commercial Nuclear Reactors

There are 99 licensed commercial nuclear reactors operating at 61 nuclear power plants in 32 States.[1] Because the Nation's nuclear power plants were built at different times by numerous vendors using different plant designs, each reactor facility is unique. However, they typically include several similar structures, systems, and components used to generate electrical power:

- **Nuclear reactor cores produce energy to heat water into steam**, which drives the turbines that operate generators to produce electrical power. Generating transformers convert the electricity into a suitable voltage for transmission to the electric grid.
- **Reactor vessels house and provide for proper control of the reactor core.** Containment structures and systems prevent the release of radioactivity into the environment if the reactor coolant system and reactor core are damaged. Pools and casks store spent nuclear fuel.
- **Heat sinks**—such as a cooling tower, river, lake, or ocean—and associated normal cooling water systems condense steam and cool plant equipment during normal operation.
- **Plant control room and reactor control systems** enable operators to control the reactor and all plant processes under normal and emergency conditions.

Five commercial nuclear power reactors are also now under construction at three sites: Vogtle nuclear power plant (Georgia, 2 units), V.C. Summer (South Carolina, 2 units) and Watts Bar 2 (Tennessee, 1 unit), where construction resumed in 2007 after being halted in 1988.[2]

Figure 1. U.S. Operating Commercial Nuclear Power Reactors



Ownership

Private utilities and public power generators own and operate all commercial U.S. nuclear power plants, though facilities may be owned by a number of separate entities and operated by a different entity than the owner. The NRC oversees and publishes information on the owners and operators of all U.S. commercial nuclear power reactors.

Safety Features and Accident Mitigation

- Nuclear power plant design and safety procedures support prevention or mitigation of damage associated with a robust series of design-basis accidents, including earthquakes, fires, floods, loss of offsite power, and extreme winds, such as hurricanes and tornadoes.

- Three distinct barriers are designed to prevent fission products from being released into the environment: the cladding that contains actual fuel pellets; the reactor vessel itself where the fuel resides, which is made of thick, high-strength steel; and the containment building that encloses the reactor components, made of heavily reinforced and specialty concrete many feet thick.
- Redundant emergency systems with redundant electrical power supplies are designed to preclude overheating, melting of the core, and release of fission products during an accident. Redundant instrumentation and control features automatically initiate reactor shutdown and emergency systems activation during an accident.
- Emergency plans and procedures and severe accident management strategies are designed to reduce accident consequences and minimize the public's radiation exposure. Training programs and frequent emergency plan testing integrated with Federal, State, and local agency involvement are designed to ensure that emergency response organizations are well prepared.

Security Features

- Nuclear power plants use defense-in-depth security, in which independent, redundant layers of defense are employed to enhance security and guard against single-point failures. Specific elements may include hardware, such as barrier and surveillance systems; procedures, including access controls, security operations, and emergency-response planning; and facility design.
- Nuclear power plants and Category I fuel cycle facilities must possess security adequate to protect against the relevant DBT. Adherence to this requirement is regularly inspected and is tested through Force-on-Force Exercises employing a mock adversary force.

Research, Training, and Test Reactors

Research, training, and test reactors (RTTRs) are non-power reactors used to conduct research, develop theoretical practices, produce radioactive sources, train nuclear engineers, and support medical applications. There are 31 small RTTRs operating in the United States, most at universities.

Figure 2. U.S. Nuclear Research and Test Reactors

RTTRs range in size from 0.1 watt to 20 megawatts (MW) thermal—in contrast to a typical commercial nuclear power reactor rated at 3,000 MW thermal. Unlike power reactors, RTTRs have only a small amount of nuclear fuel, and an accident or attack would produce only limited local effects. However, it likely would produce public panic out of proportion to the physical hazards. In cooperation with DOE's National Nuclear Security Administration (NNSA), 20 of the reactors using highly enriched uranium (HEU) fuel have been converted to the use of low enriched uranium (LEU) fuel. The NNSA is working to develop a replacement LEU fuel for the remaining five that could not be converted.[3]

Ownership

- Most are located at universities or colleges, while several others are operated by private companies or the Federal Government.

Safety Features and Accident Mitigation

- All RTTRs have automatic shutdown systems. Redundant systems initiate a reactor shutdown to protect the public during an accident or emergency.
- Most RTTRs require cooling for only short periods after a shutdown and do not generate enough heat to cause concern in a loss-of-coolant accident. Others have auxiliary features to add water from a tank or city water supply to provide core cooling.
- Many are located in pools, under enough water to provide necessary radiation shielding.

Security Features

- Because of the relatively low power output, the more extensive security requirements for power reactors are not mandated for RTTR facilities.
- Instead, the NRC imposes varying security requirements based on its evaluation of a particular RTTR's site-specific criteria, such as source-term (quantity and enrichment of special nuclear material), thermal power output, physical design, etc.
- In addition, the DOE NNSA provides voluntary security enhancements and specialized training through its Global Threat Reduction Initiative (GTRI) at domestic sites that use Category 1 and 2 radioactive sources. Entities that participate in GTRI programs must first meet all NRC and Agreement State regulatory requirements. NNSA also safely and securely recovers radiological sources that are no longer in use.[4]

Deactivated Nuclear Facilities

Decommissioning is the regulated process by which a licensed nuclear facility is safely removed from operational service while protecting radioactive materials onsite.

- 18 nuclear power reactors are in various stages of decommissioning in 12 States.[5]
- 5 power reactors have permanently shut down since 2010: San Onofre (California, 2 units), Crystal River (Florida, 1 unit), Kewaunee (Wisconsin, 1 unit), and Vermont Yankee (Vermont, 1 unit).
- 8 RTTRs are decommissioning, and 3 are permanently shut down.[6]

Fuel Cycle Facilities

Fuel cycle facilities produce fuel for nuclear power plants, research reactors, and military reactors, such as submarines. Facilities in this subsector also conduct uranium mining and milling, uranium enrichment, and uranium conversion. Fuel cycle facilities are categorized based on the types and quantities of nuclear material they store or produce—specifically high enriched uranium-235, low enriched uranium, uranium-233, or plutonium. See Appendix C for additional information on the categorization of fuel cycle facilities.

The NRC regulates **14 fuel fabrication and production facilities** (of which 6 are inactive) in 10 States[7] and **10 uranium recovery facilities** in 4 States:

- Uranium mining and milling facilities include one traditional uranium mill and nine in-situ leach extraction facilities:[8]
  - A uranium mill is a chemical plant designed to extract uranium from mined ore. The mined ore is brought to the milling facility by truck (typically from a mine within about 30 miles), and the ore is crushed and leached, producing a uranium product referred to as "yellow cake" because of its yellowish color. Most mills in the United States are being decommissioned. One is in cold shutdown mode, and one is operational.

  - In situ leaching facilities inject a leaching agent, such as oxygen with sodium carbonate, through wells into the ore body to dissolve the uranium. The leach solution is pumped from the formation, and ion exchange separates the uranium from the solution.

- Fuel cycle facilities convert, enrich, and fabricate uranium into fuel for use in nuclear reactors, and deconversion facilities process the depleted uranium hexafluoride for disposal.

Nuclear Materials Transport

A dedicated transportation infrastructure—primarily casks, trucks, rail, air, and barges—carry nuclear materials at all hazard levels, ranging from used nuclear fuel from nuclear power plants to high-volume, low-activity NORM (Naturally Occurring Radioactive Material) and technologically-enhanced NORM (TE-NORM), such as radioactive fracking and oil field waste. About 3 million packages of radioactive materials are shipped each year in the United States.[9] Regulating the safety of these shipments is the joint responsibility of the NRC, the U.S. Department of Transportation (DOT), and the Organization of Agreement States.

Vendors include the manufacturers of shipping casks and packages; shippers; manufacturers of dedicated vehicles, such as trucks designed specifically for radioactive material transport; transporters of ultra-heavy components for nuclear facilities, such as reactor vessel heads; and suppliers of tracking software.

The NRC and DOT approve packages used for shipping nuclear material based on the quantity. DOT typically regulates shipment for Type A quantities, while the NRC regulates larger Type B quantities. Most Type B packages undergo more rigorous testing and receive a Radioactive Material Package Certificate of Compliance (CoC) from the NRC. Certified packages must be shown by test or computer analysis to withstand a series of accident conditions, including high impacts, fire, and water immersion. Tests are performed in sequence to determine their cumulative effects on the package.

NRC has specific requirements for shippers of used nuclear fuel. A shipper must use NRC-approved highway routes for transport and make sure that the nuclear waste is protected against radiological sabotage. Shippers must meet specific requirements that include notifying NRC of the shipment, having procedures for addressing emergencies, having a communications center, having a written log of shipment events, making arrangements with local law enforcement agencies for shipments while en route, and using armed escorts in heavily populated areas. The time and date of the shipment must be protected as sensitive information to guard against any act that could threaten the shipment.

Radioactive Waste

Material characterized as radioactive waste includes a broad range of substances: some are highly radioactive and remain hazardous for thousands or hundreds of thousands of years, while others are radioactive and will decay to background levels within hours or days. Radioactive waste can be solid, liquid, or, less frequently, gaseous.

Nuclear power plants store nuclear waste in onsite underwater pools for at least five years, after which it can be moved to above ground dry cask storage systems. The Nuclear Sector also produces a range of radioactive wastes that must be managed in special storage or disposal facilities, all licensed and monitored by NRC or Agreement States:

- Since the Nuclear Sector does not reprocess used fuel, it is only responsible for a small amount of vitrified **high-level waste (HLW)** from a now-closed reprocessing facility that operated briefly in West Valley, New York. Vitrification of 600,000 gallons of HLW from West Valley was completed in 2002 and the stabilized waste is stored onsite.

- **Low-level waste (LLW)** is divided into three classifications (Classes A, B and C), depending on waste characteristics. A wide variety of items become LLW at the end of their useful lives. These include protective clothing; wipes; worn piping, valves, and other equipment; disused medical isotopes and carcasses from research animals injected with radioactive tracers; obsolete gauges and sources; and many more items.

- A fourth category of LLW, **Greater-than-Class-C (GTCC)**, comprises waste with radioactivity levels above those of Class C, but does not fall into the legislative definition of HLW. Waste classified as GTCC includes power reactor internal components and some high activity sealed sources. DOE is currently working to develop and obtain approval for a GTCC Environmental Impact Statement (EIS) for the disposal of GTCC wastes, including certain radioactive sealed sources.

- Waste that is both chemically hazardous and radioactive is often referred to as **mixed waste**. Some of this waste must be handled in accordance with multiple sets of government requirements for management of both hazardous wastes and radioactive wastes.

Radioactive Materials

Radioactive materials and radioactive sources are used for a wide variety of applications, including diagnostic nuclear medicine, medical therapy, life science and biomedical research, nondestructive testing, and irradiation of food and medical products. Sources vary widely in physical size and properties, the amount and kind of radioactive material they contain, and the way the material is contained.

- **Sealed sources** are those in which the radioactive material is encased in permanent shielding. They range from large, high-activity sources in fixed pieces of equipment—such as high-activity radiotherapy machines for cancer treatment and irradiators for food and medical equipment—to smaller, portable gauges used in well logging and industrial process monitoring.
- **Unsealed, short-lived radioactive material** is used in a variety of applications, including medical "cocktails" and tracers used in research.
- **Unsealed, long-lived radioactive material** is used in a variety of applications, including tracers used in research and basic sciences.

NRC or Agreement States license all sources, source users, and radioactive materials users, such as hospitals and manufacturers. Radioactive material cannot be used until the proper regulatory authority issues a license. Regulators perform periodic inspections to ensure secure storage, proper use, and protection of public health and safety.

2.2 Sector Risks

The Nuclear Sector's significant economic benefits, including provision of reliable baseload electricity, are countered by the magnitude of the consequences that could be associated with potential failure, damage, or disruption of critical assets. Many sector-specific risks are well-understood, and the sector has taken critical steps to mitigate them. The Nuclear Sector is the most closely regulated of all infrastructure sectors, and the nuclear industry has taken additional steps to protect assets, respond to and recover from incidents, and enhance resilience, particularly since the March 2011 Fukushima accident in Japan. Chapter 3 outlines the sector's risk management approach. However, evolving threats create and expose new risks that the sector has used to inform its goals, priorities, and activities in Chapter 4.

Notable Trends and Emerging Issues

Since the last SSP was issued in 2010, key changes have affected the sector's risk profile:

- **Japan's March 2011 Fukushima Daiichi accident**—The March 2011 triple meltdown at Japan's Fukushima-Daiichi nuclear power plant after a massive earthquake and tsunami illustrated a worst-case risk scenario for nuclear facilities. The meltdown resulted in evacuations that could last decades in some areas, billions of dollars in damage, additional billions of dollars in cleanup expenses, and the loss of a significant portion of Japan's electricity resources. Most of the world's nuclear facilities, including all U.S. facilities, are re-evaluating their ability to withstand beyond-design-basis events and taking steps to improve protection, response, recovery, and resilience. These include enhanced protective measures against natural disasters; enhanced backup systems, such as emergency onsite power supplies; central stores of emergency backup equipment that can be transported to any nuclear facility; new robotics and modeling technologies; and new national and international coordinated response protocols.
- **New power reactor construction**—Since 2010, two utilities have begun construction on four large power reactors, two in South Carolina and two in Georgia. Construction was restarted in 2007 on the Watts Bar 2 reactor in Tennessee, after being halted in 1988. New construction has a unique set of risks that range from supply chain interruptions to site-specific vulnerabilities.
- **Shutdown of power reactors and other facilities**—Five large power reactors have permanently shut down: San Onofre in California (2 units), Crystal River in Florida (1 unit), Kewaunee in Wisconsin (1 unit), and Vermont Yankee in Vermont (1 unit). The last remaining gaseous diffusion plant for uranium enrichment was shut down in

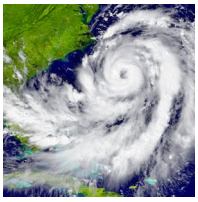
2011. Decommissioning facilities have a different risk profile from operating facilities due to the need to segment and dismantle large buildings and equipment, some of which are radioactively contaminated.

- **Aging nuclear power plants and equipment**—NRC has renewed the original operating licenses for 73 U.S. nuclear power units for an additional 20 years, increasing their allowed operating time from 40 to 60 years. Some operators already are considering life extensions to 80–100 years.
- **Climate change and increasing natural disasters**—Climate change may bring more extreme weather, reduced water tables, increasing droughts, and greater earthquake threats. It also can bring about changes in water chemistry and biota that can affect nuclear power plant operations.
- **Changing power supply and aging power grids**—The increasingly taxed electricity grid is aging, increasing the risk of widespread power outages. Post Fukushima, U.S. nuclear power plant operators have significantly increased their ability to cope with blackout conditions; but grid failures still present a major challenge, particularly when they happen suddenly or in conjunction with other natural or manmade disasters.
- **Shrinking number of medical isotope suppliers**—The United States imports more than 90 percent of its domestically consumed isotopes by volume, including its entire supply of molybdenum-99 (Mo-99).[10] About 80 to 85 percent of nuclear medicine procedures use Mo-99,[11] which is produced by five aging reactors in Canada, Europe, and South Africa. Two reactors that provide about 90 percent of the world's Mo-99—the NRU reactor in Canada and the HFR reactor in the Netherlands—are both more than 50 years old and are slated to shut down in 2016 or soon after.[12] NRU was shut down for more than a year from 2009-2010 for maintenance, creating a significant shortage in the United States and Europe. The NRC is currently working with two separate companies on proposed applications for Mo-99 utilization facilities in Wisconsin and Florida. In addition, NorthStar Medical Radioisotopes LLC in Madison, Wisconsin, is working to create instrumentation and associated disposables for radionuclide separation, dosing, and dispensing for sale to research laboratories and commercial suppliers.
- **Increasingly sophisticated cyber threats**—The Nuclear Sector faces multiple, rapidly changing cyber threats, including hackers' evolving ability to gain control of control technologies and computer-enabled vehicles, medical devices, small drones, and other items; state-sponsored industrial espionage; Internet-based financial tampering; embedded malware in critical infrastructure hardware components; and supply chain attacks. Three-dimensional printing presents both potential risks and protective applications. A 3-D printer can produce both weapons and defective parts, but it also can be used to quickly replace a failed part such as a valve component.

Significant Nuclear Sector Risks

A significant incident or failure at a major nuclear facility would likely result in extremely high economic costs, major onsite and/or offsite property damage, and evacuations. It also would result in long-term cleanup costs and economic damage to the local region. The consequences of an incident at a nuclear facility would depend on a number of factors, including the nature of the facility, the asset's critical functions, system redundancies, the kind and amount of radioactive material at the site, the location, downstream population density, regional infrastructure, and seasonal and weather conditions. The following list identifies the key risks affecting the security and resilience of Nuclear Sector assets, operations, and workforce.

Natural Disasters and Extreme Weather



Droughts can decrease the water levels in rivers, lakes, and canals that provide cooling water for nuclear power plants. Some nuclear power plants have had to shut down temporarily during drought conditions because the water level was below cooling water intake pipes, the water temperature exceeded allowable temperatures for cooling water intake, or water had become so brackish or algae-laden that it would have clogged cooling system equipment.

Major storms, earthquakes, and tsunamis can severely damage critical operating and emergency equipment. These risks are taken into consideration during the construction and maintenance of each facility.

Structural Issues

Because of the highly specialized design of nuclear power plants, design or construction flaws that are not discovered in advance can jeopardize plant operations. Past issues have included generators that fail after only a few years, structural damage due to construction, and corrosion.

Quality control systems for components from U.S. and international suppliers are a part of plant operations.

Aging Infrastructure and Workforce

The average operating life of U.S. nuclear power plants is 40 years. All of the current-generation U.S. power reactors were essentially "custom built," and, in some cases, the original specifications, organizational knowledge, or components may no longer be available or may be incompatible with more recent systems.

Other nuclear assets also are aging. The only U.S. uranium conversion plant was built in the 1950s. Several research reactors were built more than 50 years ago.

More than 120,000 people work in the U.S. nuclear industry and approximately 38 percent will be eligible to retire within five years. The nuclear industry has focused extensively on retaining the institutional knowledge base and transmitting it to younger workers.

Deliberate Attacks and Terrorism

The NRC and the U.S. nuclear industry have prepared extensively for nuclear power plants to protect against the DBT for each facility. Nuclear power plants continue to evaluate and protect facilities against the threat of targeted large-scale terrorist attacks, which, if successful, could potentially lead to contamination within the surrounding community, widespread power disruptions, or injuries and damage.

Emerging concerns include small, unmanned drone aircraft and other types of remotely operated vehicles that could be used for surveillance or to launch small-scale attacks.

Individual or small group attacks launched by disgruntled individuals or activists can also create potential disruptions. Past incidents have included individuals using high-powered weapons from outside of the plant perimeter to shoot at large structures, such as cooling towers. Robust facility design, construction, and maintenance mitigates this issue.

Cyberattacks

The Nuclear Sector faces multiple, rapidly changing cyber threats from both within the United States and abroad. These include hackers' evolving ability to gain control of computer-enabled vehicles, medical devices, small drones, and other items; state-sponsored industrial espionage; Internet-based financial tampering; embedded malware; and supply chain attacks.

NRC's comprehensive cybersecurity regulations require each facility to maintain a robust cybersecurity plan. DHS has also conducted an internal review of nuclear cyber risks and dependencies.

Supply Chain Disruptions

All U.S. nuclear facilities rely heavily on international suppliers for key replacement components and critical systems, such as software, training simulators, etc. Some components, such as heavy forgings for reactor vessels, are only available from one or a very limited number of overseas suppliers. Nuclear facilities are also dependent on supply chains for the transport of uranium from mills and other fuel cycle facilities and medical isotope supplies. A disruption in the supply of fuel, depending on its duration, could affect operations.

Source Diversion or Mishandled and "Orphan" Radioactive Sealed Sources

Orphan radioactive sealed sources include older sources that were never regulated and those that were abandoned, lost, misplaced, stolen, or removed without authorization. Orphan radioactive sealed sources introduce the risk of accidental or inadvertent misuse or destructive acts that can expose unknowing individuals.

Mishandling sources, including the inadvertent melting of radioactive sources, can create health concerns for the individuals immediately involved and require expensive cleanup.

The Center for Nonproliferation Studies (CNS) identified 325 incidents in 38 countries related to the loss, theft, or trafficking of radioactive sealed sources in 2013 and 2014.[13] This figure only includes publicly reported incidents, and it is likely that more incidents occur annually.

Terrorists may steal or divert sources to create radiological dispersal devices (RDDs), which are intended to spread radioactive material with malicious intent. The International Atomic Energy Agency (IAEA) has an Incident and Trafficking Database (ITDB) that contains information, reported and confirmed by more than 70 nations, on the black market trade in radioactive sources and unsealed radioactive materials.

Primary Cross-Sector Interdependencies

Lifeline Functions: Energy, Transportation Systems, Communications, and Water

Nuclear facilities both supply electricity to the grid and depend heavily on uninterrupted power for continuous safe operation. Nuclear power plants employ multiple backup generation systems and adhere to detailed regulations governing safe shutdown in the event of long-term local grid failure and loss of offsite power. Grid interdependencies have become a higher priority post-Fukushima, where the extended loss of AC power threatened core cooling and containment integrity. The Oil and Natural Gas Subsector also relies on nuclear materials and byproducts for well logging, a process used in oil and gas exploration.

Nuclear and radioactive materials are shipped nationally and internationally via ships, barges, trains, trucks, and airplanes. Transportation disruptions could hinder the movement of materials to nuclear sites or end users, causing cascading disruptions to site operations or in sectors that depend on nuclear materials. The sector also relies on airport screening and security measures to protect nuclear infrastructure against air attacks. Transportation failures resulting from natural or manmade disasters could leave a nuclear facility without access to equipment, food, and medical care for employees for an extended period of time. The Transportation Systems Sector also uses nuclear density gauges during road construction to ensure that roads meet DOT standards.

Communications—both onsite and with critical public and private partners—are essential during an emergency to ensure effective response and maintain public safety. Nuclear facilities rely on uninterrupted Internet and communications networks for both efficient operations and timely information sharing.

More than half of U.S. nuclear power plants use once-through cooling, in which large quantities of water (about 90 cubic meters/second for a 1,600 megawatt equivalent nuclear power plant) are are withdrawn from a large river, lake, or the ocean; treated; and used to cool the secondary steam circuit before being returned to the source. Water used to cool the reactor core itself is contained in a closed loop and never released to the environment in other than accident conditions. A water shortage or change in the temperature or chemistry could significantly hinder and, in some circumstances, stop operations at nuclear power plants.

Key Interdependencies

Radioactive materials support multiple medical applications to monitor, image, or treat metabolic processes or tissues in humans. The United States performs about 17 million medical procedures each year using radioactive materials[14]—and the U.S. now imports more than 90 percent of its domestically consumed isotopes by volume, including its entire supply of molybdenum-99 (Mo-99).[15] About 80 to 85 percent of nuclear medicine procedures use Mo-99, though long-term continued supply is uncertain.[16] In turn, the Nuclear Sector relies on healthcare to ensure workforce health and safety against pandemic diseases.

Information technology systems control critical processes, manage day-to-day operations, and store sensitive information in the Nuclear Sector. Protecting critical process control systems from cyberattack is a high sector priority. The Nuclear Sector and its industry and government partners also use IT services to facilitate information sharing and dissemination of security and threat data.

Federal, State, and local emergency responders have defined roles to play in any emergency involving a nuclear facility or radioactive materials. Events that may require emergency services include loss or theft of radioactive materials or sources, contaminated air or water releases from a nuclear facility, fires, breaches of the security perimeter, laboratory or test facility accidents, transportation accidents involving nuclear materials, and major nuclear accidents or malevolent acts that require evacuation and long-term decontamination.

The principal hazard to public health and safety during an accident at a fuel cycle facility would be from the release of onsite chemicals. Chemicals are used daily in the production of electricity at commercial power plants.

The Nuclear Sector relies on the Critical Manufacturing Sector for a wide range of key plant components including piping, valves and valve components, electrical cable, shielding materials, etc. Some large, highly specialized components, such as replacement reactor vessel heads, are available only, or primarily from overseas suppliers.

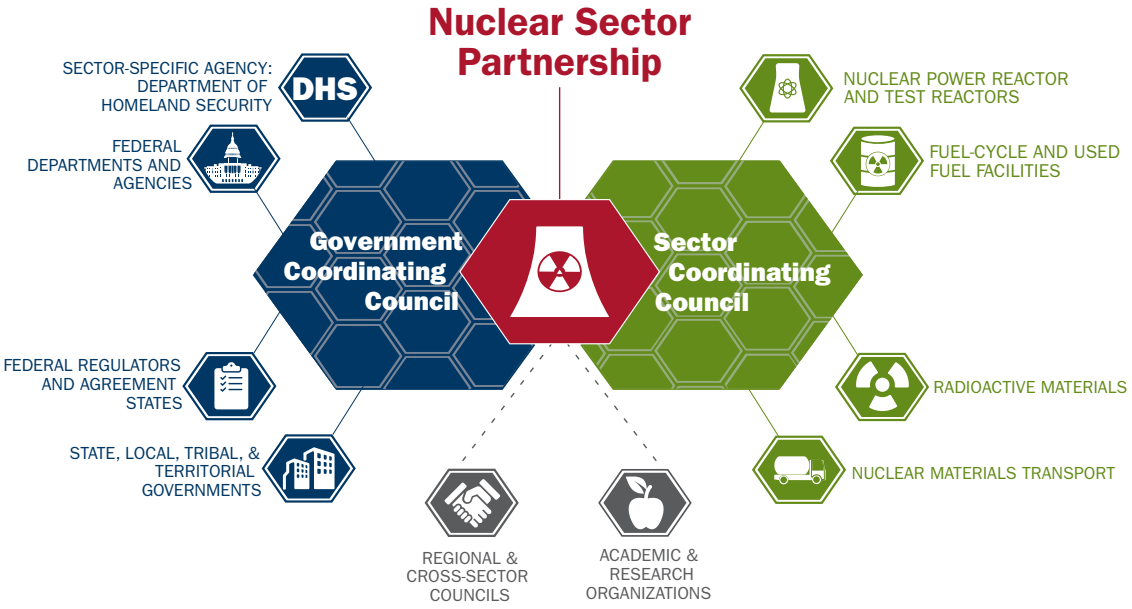
The Federal Government is required to create an inventory of infrastructure outside the United States that, if disrupted or destroyed, would lead to loss of life in the United States or would critically affect the Nation's economic, industrial, or defensive capabilities. In response, DHS, working with the Department of State, developed the Critical Foreign Dependencies Initiative (CFDI), an effort designed to ensure that a classified National Critical Foreign Dependencies List will be inclusive, representative, and leveraged in a coordinated and responsible manner.

2.3 Critical Infrastructure Partners

Voluntary collaboration between private sector and government stakeholders has been and remains the primary mechanism for advancing collective action toward Nuclear Sector security and resilience. Like all 16 critical infrastructure sectors, the Nuclear Sector operates under the NIPP 2013 partnership structure, which encourages participation from the private sector; government partners at Federal, State, local, and regional levels; and academic and nongovernmental organizations that support sector security and resilience.

Nuclear Sector Partnership Structure

Figure 3. Nuclear Sector Partnership Structure



The NIPP 2013 partnership structure includes representative public and private sector councils that operate under the Critical Infrastructure Partnership Advisory Council (CIPAC) construct. CIPAC facilitates interaction between the community of owners and operators and the sector's Federal, State, local, tribal, and territorial government representatives to conduct deliberations and form consensus positions for the Federal Government.

The Nuclear Sector partnership includes the full community of hundreds of U.S. owners and operators, represented by the members of the Sector Coordinating Council (SCC) and Government Coordinating Council (GCC). The success of the Nuclear Sector partnership depends on the ability to leverage the full spectrum of capabilities, expertise, and experience from the sector and its stakeholders through the partnership councils. It also depends on the members' ability to share information, guides, tools, and best practices out to their networks of stakeholders who do not sit on partnership councils.

Partnership councils meet regularly to exchange ideas and lessons learned, facilitate sector-level planning and resource allocation, establish effective coordinating structures, and develop security and resilience tools, guidelines, products, and programs. Partnership councils are described below. An updated list of council members and their charters can be found on the Nuclear Sector Council Charters and Membership Webpage.

Sector-Specific Agency

Sector coordination is led by the U.S. Department of Homeland Security, which functions as the Sector-Specific Agency (SSA), and serves as the primary Federal interface for sector-specific security and resilience efforts, promotes sector-wide information sharing, and supports implementation of the NIPP 2013 within the Nuclear Sector.

The Office of Infrastructure Protection (IP) fulfills the role of SSA on behalf of DHS. The Assistant Secretary for IP chairs the Nuclear GCC, and has designated the Director of the Sector Outreach and Programs Division (SOPD) as the representative on behalf of DHS IP. The SOPD Director designates an alternate to assist as necessary.

Nuclear Government Coordinating Council

The Nuclear GCC enables interagency, intergovernmental, and cross-jurisdictional coordination on security and resilience strategies, activities, and policies. Members include:

Conference of Radiation Control Program Directors (CRCPD)

CRCPD is a 501(c)(3) nonprofit, nongovernmental professional organization dedicated to radiation protection. Its mission is to promote consistency in addressing and resolving radiation protection issues, to encourage high standards of quality in radiation protection programs, and to provide leadership in radiation safety and education.

Customs and Border Protection (CBP)

As the Nation's primary border enforcement agency, CBP must do everything in its power to prevent terrorists and terrorist weapons, including weapons of mass destruction, from entering the United States. CBP must fulfill this mission while simultaneously facilitating the flow of legitimate trade so vital to the U.S. economy. Nuclear and radiological materials are of particular concern because of their potential to harm large numbers of people and disrupt the U.S. economy.

Domestic Nuclear Detection Office (DNDO)

DNDO plays an essential role in developing and implementing a defensive strategy with domestic and international programs to protect the Nation from a nuclear or radiological terrorist attack. DNDO is the primary agency within the U.S. Government responsible for developing the global nuclear detection architecture. It supports the deployment of the domestic detection system to detect and report attempts to import or transport a nuclear device, fissile, or radiological material intended for illicit use.

Federal Bureau of Investigation (FBI)

The FBI enforces statutes aimed at preventing criminal and terrorist activity involving nuclear and radioactive material, in addition to its overarching terrorism response authorities outlined in various National Security, Presidential Policy, and Homeland Security Presidential Directives. The FBI also supports collaborative exercises that test response capabilities to incidents involving radiological materials.

Federal Emergency Management Agency (FEMA)

FEMA takes lead responsibility for all offsite nuclear planning and response.

Nuclear Regulatory Commission (NRC)

NRC regulates the civilian nuclear industry, including commercial nuclear power plants; non-power reactors for research and testing; nuclear materials used in medicine, industry, and research; fuel cycle facilities; and transportation, storage, and disposal of nuclear materials, used nuclear fuel, and waste. NRC is an independent agency headed by a five-member commission that formulates policies, develops regulations, issues orders to licensees, and adjudicates legal matters.

Organization of Agreement States (OAS)

The membership of OAS consists of state radiation control directors and staff from the 37 Agreement States who are responsible for implementation of their respective Agreement State programs. The purpose of the OAS is to provide a mechanism for these Agreement States to work with each other and with the NRC on regulatory issues associated with their respective agreements.

State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC)

The SLTTGCC strengthens the sector partnership by bringing together experts from a wide range of professional disciplines that relate to critical infrastructure security from all levels of government. The SLTTGCC supports geographically diverse partnerships to ensure that State, local, tribal, and territorial officials play an integral role in national critical infrastructure protection and resilience efforts.

Transportation Security Administration (TSA)

The TSA is responsible for strengthening the security of the Nation's transportation systems. TSA uses a risk-based strategy and works closely with transportation, law enforcement, and intelligence communities to set the standard for excellence in transportation security.

U.S. Coast Guard (USCG)

The USCG safeguards our Nation's maritime interests and environment around the world. USCG is an adaptable, responsive military force of maritime professionals whose broad legal authorities, capable assets, geographic diversity, and expansive

partnerships provide a persistent presence along our rivers, in the ports and littoral regions, and on the high seas. It is responsible for maritime safety, security, and environmental stewardship.

U.S. Department of Defense (DOD)/Defense Threat Reduction Agency (DTRA)

DTRA is the DOD's official Combat Support Agency for countering weapons of mass destruction and addresses the entire spectrum of chemical, biological, radiological, nuclear, and high-yield explosive threats.

DOD/Homeland Defense & America's Security Affairs

This division is responsible for the supervision of DOD homeland defense activities, defense support of civil authorities, and Western Hemisphere security affairs for the Department of Defense.

DOD/U.S. Northern Command (USNORTHCOM)

USNORTHCOM partners to conduct homeland defense, civil support, and security cooperation to defend and secure the United States and its interests. USNORTHCOM's civil support mission includes domestic disaster relief operations that occur during fires, hurricanes, floods and earthquakes. Support also includes counter-drug operations and managing the consequences of a terrorist event employing a weapon of mass destruction.

U.S. Department of Energy (DOE)

DOE promotes research, development, and other activities to support nuclear power development and the use of byproduct, source, and special nuclear materials for energy, medical, biological, research, and other uses.

DOE/National Nuclear Security Administration (NNSA)

The NNSA's Global Threat Reduction Initiative (GTRI) supports the DOE Nuclear Security Goal of reducing the risk of terrorists acquiring nuclear and radiological materials that could be used in weapons of mass destruction (WMDs) or other acts of terrorism.

U.S. Department of Health and Human Services (HHS)

HHS is the U.S. Government's principal agency for protecting the health of all Americans and providing essential health services.

U.S. Department of Homeland Security (DHS)

DHS leads Federal coordination with the private sector as the Nuclear SSA and chair of the Nuclear GCC.

U.S. Department of State

Two offices in the State Department's Bureau of International Security and Nonproliferation support international engagement for critical infrastructure protection:

- **Office of Nuclear Energy, Safety, and Security** leads development of U.S. policy on peaceful nuclear cooperation, nuclear energy, nuclear export controls, and the physical protection of nuclear materials and facilities to further U.S. nuclear nonproliferation and energy goals.
- **Office of Weapons of Mass Destruction Terrorism** enhances international security against the threat of WMD terrorism by strengthening political and operational capability of international partners to deter, detect, defeat, and respond to terrorists and their facilitators. This includes diplomatic support and leading coordination activities involving several U.S. efforts to counter nuclear smuggling and promote nuclear forensics cooperation with foreign partners—which leverage U.S. expertise to advance broader counterterrorism and nonproliferation goals.

U.S. Department of Transportation (DOT)

The Secretary of Transportation has the regulatory and enforcement authority to enhance the safe transportation of hazardous materials by all modes and hazardous liquids and natural gas by pipeline. The Secretary also has the authority to marshal transportation in a defined area to aid in national defense and homeland security.

U.S. Environmental Protection Agency (EPA)

EPA uses its authority from the Clean Air Act to limit the amount of radioactive material released into the air from nuclear facilities. EPA sets limits on radioactive emissions from all Federal and industrial facilities. EPA also limits the amount of radiation from the disposal of spent nuclear fuel and high-level radioactive waste.

Nuclear Sector Coordinating Council

The Nuclear SCC is a self-organized, self-governed council of private sector owners and operators and industry association that coordinate on strategy, policy, information sharing, and risk management activities. Members include:

- Dominion Generation
- Exelon Generation Company, LLC
- Harvard University/Boston Children's Hospital
- Mallinckrodt Pharmaceuticals
- Nuclear Energy Institute
- Oregon State University
- Reed College
- Rutgers University
- Security Engineering Associates
- University of Missouri

While the precise makeup of the Nuclear SCC may change, it will generally conform to the following guidelines:

- Six members from companies owning or operating at least one commercial power reactor.
- One member from owners of fuel manufacturing or fuel fabrication facilities.
- One member from manufacturers of nuclear reactors or components.
- One observer from the National Organization of Test, Research, and Training Reactors (TRTR).
- One member from a nuclear waste management or transportation company.
- One member from the Nuclear Energy Institute (NEI). NEI is a member because it represents a large portion of the overall sector. All domestic operators of commercial nuclear power plants and fuel processing facilities are members of NEI. Through NEI, the industry can undertake initiatives that commit the entire industry to specific action.
- Representative(s) from the Nuclear Sector Coordinating Council-Radioisotopes Subcouncil (NSCC-R).

Nuclear Energy Institute (NEI)

NEI is the leading U.S. nuclear industry trade association. All U.S. nuclear power plant operators are members of NEI, as are many materials licensees. NEI provides the political and policy interface for the industry and represents the various segments of the nuclear industry in communicating questions or concerns to the NRC. Working groups and task forces organized through NEI provide information exchange and establish performance guidelines on topics ranging from security to fire protection. NEI and the industry established the Security Working Group (SWG) to provide guidance and oversight of industry activities concerning cyber and physical security. The SWG comprises industry security managers and executives and meets frequently to coordinate and optimize security efforts. The SWG provides the means for industry to strategically approach improvements to its risk posture.

Nuclear Sector Working Groups and Subcouncils

Nuclear SCC Radioisotopes (NSCC-R) Subcouncil

NSCC-R consists of members representing the broad security interests of the radioisotope industry. The subcouncil has representatives from companies in the United States that are licensed to operate radioisotope manufacturing, handling, or processing facilities; companies in the United States that are licensed to distribute radioisotope products; and others involved in the nuclear industry. The mission of the subcouncil is to develop and recommend strategies that will enhance the physical security and emergency preparedness of the radioisotope industry under the auspices of the NIPP. The NSCC-R works closely with the Nuclear GCC Radioisotopes Subcouncil in fulfillment of this objective.

Nuclear GCC Research and Test Reactor Subcouncil (NGCC-RTR)

NGCC-RTR coordinates security strategies, policies, activities, and communications across the U.S. Government and between the U.S. Government and the RTR community. The subcouncil also coordinates with emergency management and public health and safety communities with regard to security and emergency preparedness in the RTR subsector. Members include DHS, NNSA, FBI, and NRC.

Nuclear SCC Research and Test Reactor Subcouncil (NSCC-RTR)

The corresponding NSCC-RTR addresses the security issues associated with research, test, and training reactors, with a primary focus on university facilities. The NSCC-RTR's primary member is the TRTR, which represents U.S. RTR facilities operated by the government, major universities, national laboratories, and private industry. Both the NSCC-RTR and NGCC-RTR coordinate implementation of programs seeking to harden RTR facilities beyond the regulatory baseline.

Joint Nuclear GCC/Nuclear SCC Cyber Subcouncil

The Nuclear GCC/Nuclear SCC Cyber Subcouncil comprises stakeholders with primary responsibility for cybersecurity in the Nuclear Sector. Members, including DHS, FBI, NRC, and private sector representatives, identify cybersecurity risks potentially affecting the Nuclear Sector and serve as a forum to share relevant information within the CIPAC framework. Members also coordinate Nuclear Sector participation in cross-sector bodies such as the Cross-Sector Cyber Security Working Group (CSCSWG) and Industrial Control Systems Joint Working Group (ICSJWG).

Additional Nuclear Sector Agency, Organization, and Program Partners

Institute of Nuclear Power Operators (INPO)

INPO includes all U.S. nuclear power plant operators. INPO provides oversight of the industry to enhance nuclear power plant safety and reliability primarily through the cornerstone programs of onsite evaluations of each nuclear power plant, training and accreditation, events analysis and information exchange, and assistance.

Atlanta Center of the World Association of Nuclear Operators (WANO)

WANO is co-located with INPO. Formed by the international nuclear community, WANO promotes worldwide improvements in the quality of nuclear power plant operations. The Atlanta Center is one of its five worldwide regional centers. INPO provides operational support and facilities for the Atlanta Center and represents U.S. nuclear utility membership in WANO.

World Institute for Nuclear Security (WINS), Vienna, Austria

Formed in 2008, WINS was modeled after WANO as an international forum for nuclear security professionals to discuss and exchange information on best security practices.

Nuclear Safety Review Committees

Each nuclear power plant has a safety review committee that provides additional independent nuclear power plant oversight. The committees, which report to senior utility management, independently review activities to provide additional assurance that the units are operated and maintained according to the operating licenses and applicable nuclear safety regulations. They also provide independent advice on the broad aspects of nuclear safety and operational performance.

Other Industry Organizations

Nuclear SCC and GCC members frequently participate in or partner with organizations and standards committees, including:

- American Concrete Institute (ACI)
- American Nuclear Society (ANS)
- American National Standards Institute (ANSI)
- American Society of Civil Engineers (ASCE)
- American Society of Mechanical Engineers (ASME)
- American Society for Non-Destructive Testing (ASNT)
- Council on Radionuclides and Radiopharmaceuticals
- Electrical Power Research Institute (EPRI)
- Health Physics Society (HPS)

- Institute of Electrical and Electronics Engineers (IEEE)
- Institute of Nuclear Materials Management (INMM)
- Society for Nuclear Medicine

Value Proposition for Participation in the Sector Partnership

Nuclear SCC members that actively participate in the sector partnership receive valuable benefits and help demonstrate the sector's commitment to security and resilience in a number of ways:

- Proprietary or business-sensitive infrastructure information can be shared with government entities that share the private sector's commitment to a more secure homeland.
- Information sharing will result in better identification of risks and vulnerabilities, which will help industry partners with others to protect key assets.
- Industry is helping to prevent disruption to the U.S. economy and way of life.
- Private industry is demonstrating good corporate citizenship that may save lives and protect communities.
- The nuclear industry recognizes that a successful attack on a nuclear facility would be devastating to the industry; therefore, it is in their best interest to detect and deter an attack before it occurs, or should one occur, to successfully defend against it.

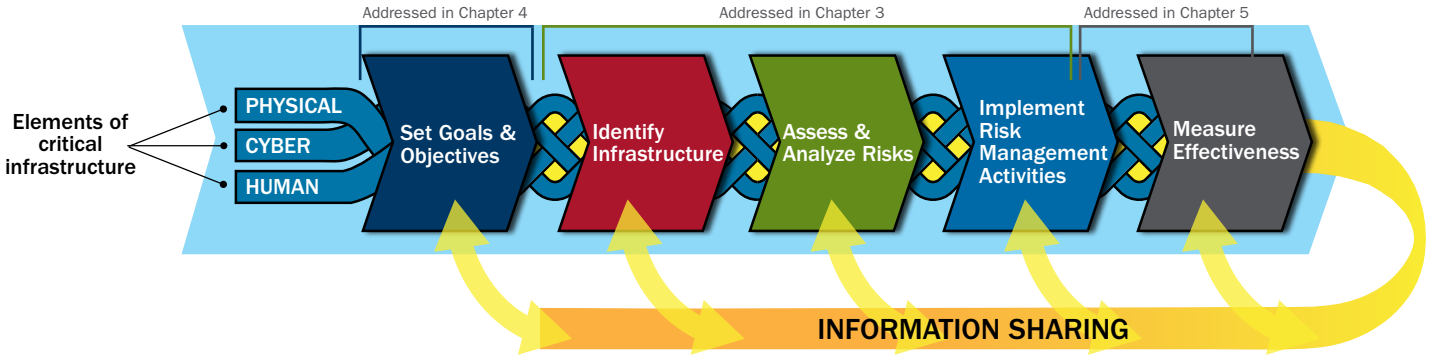
CHAPTER ENDNOTES

1. U.S. Nuclear Regulatory Commission (NRC), "Operating Reactors: What We Regulate," last updated February 18, 2015, http://www.nrc.gov/reactors/operating.html; U.S. Nuclear Regulatory Commission (NRC), "List of Power Reactor Units," last updated May 15, 2014, http://www.nrc.gov/reactors/operating/list-power-reactor-units.html.
2. U.S. Nuclear Regulatory Commission (NRC), "Combined License Holders for New Reactors," last updated September 19, 2013, http://www.nrc.gov/reactors/new-reactors/col-holder.html.
3. National Nuclear Security Administration, "GTRI's Convert Program: Minimizing the Use of Highly Enriched Uranium," last updated May 29, 2014, http://www.nnsa.energy.gov/mediaroom/factsheets/gtri-convert.
4. National Nuclear Security Administration, "NNSA: Securing Domestic Radioactive Material," last updated May 29, 2014, http://nnsa.energy.gov/mediaroom/factsheets/gtri-protect.
5. National Nuclear Security Administration, "GTRI's Convert Program: Minimizing the Use of Highly Enriched Uranium," last updated May 29, 2014, http://www.nnsa.energy.gov/mediaroom/factsheets/gtri-convert.
6. U.S. Nuclear Regulatory Commission (NRC), "Backgrounder on Research and Test Reactors," last updated December 12, 2014, http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/research-reactors-bg.html.
7. U.S. Nuclear Regulatory Commission (NRC), "Locations of Major U.S. Fuel Cycle Facilities," last updated April 2, 2015, http://www.nrc.gov/info-finder/materials/fuel-cycle/.
8. U.S. Nuclear Regulatory Commission (NRC), "Locations of Uranium Recovery Facilities," last updated April 2, 2015, http://www.nrc.gov/info-finder/materials/uranium/.
9. U.S. Nuclear Regulatory Commission (NRC), "Materials Transportation," last updated February 10, 2015, http://www.nrc.gov/materials/transportation.html.
10. U.S. International Trade Commission, *Stable and Radioactive Isotopes: Industry & Trade Summary* (Office of Industries, June 2009), http://www.usitc.gov/publications/332/ITS-1.pdf.
11. TRIUMF, *Making Medical Isotopes: Report of the Task Force on Alternatives for Medical-Isotope Production* (TRIUMF, 2008), http://www.triumf.ca/sites/default/files/Making-Medical-Isotopes-PREPUB.pdf.
12. Puthenedam, Manjula, "Lessons Learned from the Moly Shortage: Is the Crisis Over?" *Molecular Imaging*, October 4, 2010, http://www.molecularimaging.net/topics/practice-management/quality/lessons-learned-moly-shortage-crisis-over.
13. James Martin Center for Nonproliferation Studies, Nuclear Threat Initiative, *CNS Global Incidents and Trafficking Database: 2014 Annual Report* (Center for Nonproliferation Studies, April 2015), http://www.nti.org/media/pdfs/global_incidents_and_trafficking2015_2.pdf?_=1430242792.
14. Society for Nuclear Materials, *Imaging with CARE* (Society for Nuclear Materials, n.d.), accessed May 2015, http://interactive.snm.org/docs/Care_report.pdf.
15. U.S. International Trade Commission, *Stable and Radioactive Isotopes: Industry & Trade Summary* (Office of Industries, June 2009), http://www.usitc.gov/publications/332/ITS-1.pdf.
16. TRIUMF, *Making Medical Isotopes: Report of the Task Force on Alternatives for Medical-Isotope Production* (TRIUMF, 2008), http://www.triumf.ca/sites/default/files/Making-Medical-Isotopes-PREPUB.pdf.

3 RISK MANAGEMENT AND NATIONAL PREPAREDNESS

Risk management is the cornerstone of the NIPP 2013 and of the national effort to strengthen security and resilience. It focuses on enabling owners and operators to make risk-informed decisions that best allocate limited resources to the most effective mitigation solutions. The NIPP 2013 outlines a critical infrastructure risk management framework (Figure 4) that enables the critical infrastructure community to focus on those threats and hazards that are likely to cause harm and to employ prioritized approaches that are designed to prevent or mitigate the effects of those incidents. It also increases security and strengthens resilience by identifying and prioritizing actions to ensure continuity of essential functions and services during incidents and support rapid response and restoration.

Figure 4: NIPP 2013 Critical Infrastructure Risk Management Framework



The Nuclear Sector goals and priorities in Chapter 4 are directly rooted in the NIPP risk management framework. Updated goals and priorities reflect the maturation of the partnership and the significant progress made since the 2010 Sector-Specific Plan. This chapter summarizes the sector's ongoing efforts and planned approaches that support risk management and national preparedness, response, and recovery following an incident that affects Nuclear Sector operations. It is important to note that a large portion of the sector's risk management activities discussed here in Chapter 3 are required by NRC regulations, and are not voluntary. Sector partners have also supplemented regulated risk management activities with voluntary activities, including information sharing, training, voluntary security enhancements, and investigation of non-radioactive alternative technologies. While this chapter discusses both regulatory and non-regulatory Nuclear Sector efforts, the forward-looking activities in Chapter 4 represent only voluntary Nuclear Sector efforts beyond what will be accomplished by regulation. For more information on sector resources, visit the Nuclear Sector Webpage or email NuclearSSA@HQ.DHS.GOV.

3.1 Risk Management

Under the NIPP 2013 framework, risk is the potential for an adverse outcome from an event, determined by the event's likelihood—a function of the specific threats and vulnerabilities—and associated consequences if the event occurs. While individual owners and operators are responsible for managing risk to their individual assets, collaborative Nuclear Sector partnership activities can improve understanding of threats, vulnerabilities, and consequences and provide owners and operators with tools, guidelines, information, best practices, and resources to facilitate more effective risk assessments and risk management decisions at the facility and sector level.

The Nuclear Sector is atypical among critical infrastructure sectors in that NRC and Agreement States license civilian use of all risk-significant nuclear and radioactive facilities in the United States. The Nuclear Sector has developed a relatively large body of information to inform the risk profile of sector assets, systems, and networks.

Significant domestic and international research has been done over the past 50 years on the risks of nuclear and radiologic facilities and materials. This research has informed, and continues to inform, determinations by owners and operators, NRC, DHS, DOE, and other sector partners on risk-significant facilities and materials and how best to mitigate risks.

Identify Infrastructure

The Nuclear Sector is distinct in that every asset is under regulation by the NRC or a delegated Agreement State. Nuclear Sector assets are well identified, well tracked, and given risk categorizations that inform which safety and security regulations they are subject to (see Chapter 2 for details on Nuclear Sector components and how they are managed). As part of their license conditions, all nuclear facilities and nuclear materials users are required to take steps to minimize safety and security risks to the facility and the nuclear material it contains, and to protect workers, the public, and the environment from radiation releases. High-hazard nuclear facilities, such as nuclear power plants, are also required to take extensive steps to minimize impacts of all foreseeable accidents or attacks.

The exception is older, "orphan" radioactive sealed sources—many pre-dating the 1974 creation of the NRC—that were lost, stolen, or abandoned. The NRC and DOE are making a concerted effort to identify and locate these sources for safe storage or disposal and to prevent the loss, diversion, or illicit trafficking of radioactive sources.

In August 2014, the NRC-led interagency **Task Force on Radiation Source Protection and Security** submitted its third report, *The Radiation Source Protection and Security Task Force Report*, to evaluate and provide recommendations relating to the security of radiation sources in the United States from potential terrorist threats, including acts of sabotage, theft, or use of a radiation source in a radiological dispersal device. (Previous reports were submitted in 2006 and 2010.) The 2014 report highlighted key areas of progress since 2010, including expanded disposal capacity, increased physical protection of byproduct material through new NRC rules, enhanced tracking and accounting, increased public education and preparedness, improved transportation security coordination, and heightened international activity and visibility.

In May 2013, NRC completed its three-part **Web-based Integrated Source Management Portfolio** which supports the Radioactive Materials Security Program and related NRC radioactive materials licensing and tracking activities:

- Web-based Licensing System (WBL), deployed in August 2012, supports the entry of licensing information that enables NRC and Agreement States to manage the licensing life cycle from initial application through license issuance, amendment, reporting, and termination. In addition to use by NRC, WBL can be used as a licensing system by those in Agreement States that choose to use it.
- License Verification System (LVS), deployed in May 2013, is a web-based system designed to enable licensed users to electronically verify the validity of a license issued by NRC or an Agreement State. Any licensee transferring Category 1 or 2 quantities of radioactive sources to another licensee, prior to conducting such transfer, must verify with the LVS or the applicable regulatory agency that the transferee's license authorizes the type, form, and quantity of radioactive material to be transferred.
- National Source Tracking System (NSTS), deployed in 2009, is a highly secure computer system that tracks high-risk radioactive sources from manufacture or import through disposal, export, or until they decay enough to no longer be of concern. The NSTS enhances the ability of the NRC and the Agreement States to conduct inspections and investigations, communicate information to other government agencies, and verify legitimate ownership and use of national tracked sources.

The United States also participates in the **International Atomic Energy Agency's (IAEA) Incident and Trafficking Database (ITDB)**, which facilitates the exchange of information among member nations on the black market trade in radioactive sources and unsealed radioactive materials reported and confirmed by more than 70 nations.

EPA and DOE's Oak Ridge National Laboratory have investigated technologies to improve tracking and monitoring of radiological materials, including sources, through real-world testing of the **Radiological Source Tracking and Monitoring (RadSTraM)** system. RadSTraM is part of a larger program, called the Integrated Safety & Security Enforcement & Interdiction System (ISSEIS), designed to increase security and reduce losses of radioactive sealed sources.

The Sector-Specific Agency for the Nuclear Sector is the U.S. Department of Homeland Security, which helps identify and obtain appropriate data for assets, systems, and networks that play a vital role in the Nation's security or economy, particularly those that involve significant dependencies, interdependencies, or critical functionality. Data collection, compilation, and storage efforts ensure that data content, accuracy, currency, and formats are standardized.

Assess and Analyze Risks

Nuclear power plant owners and operators have generally supported risk-informed approaches to safety and security, both in fulfilling regulatory requirements and voluntarily improving safety and security. NRC and the Nuclear Sector work together to assess and analyze risks from both natural and manmade threats, including deliberate attacks and sabotage of nuclear facilities and materials.

The extent and sophistication of risk assessment has increased in the wake of several high-profile events worldwide over the past 35 years. Chief among these are the 1979 Three Mile Island meltdown in Pennsylvania, the 1986 Chernobyl explosion in the former Soviet Union, the 2001 terrorist attacks on the United States, and the 2011 triple meltdown at Japan's Fukushima Daiichi nuclear power plant in the wake of a massive earthquake and tsunami.

NRC has used **probabilistic risk assessments** (PRAs) for more than 30 years to analyze risk to its licensees. PRA is a systematic process for examining how engineered systems, such as nuclear power plants, and human interactions with these systems work together to ensure safety and security. In 1995, NRC adopted a PRA policy statement that directed increased use of state-of-the-art PRA methods in all regulatory matters to complement NRC's deterministic approach and support the traditional defense-in-depth philosophy.

The deterministic approach seeks to answer two questions: What can go wrong? What are the consequences? PRA seeks to answer a third question: How likely is it that something will go wrong? Applying this third question is known as risk-informing the process. By risk-informing its analyses, NRC can focus regulatory effort on protecting the public from events that result in significant adverse consequences or that are more likely to occur.

RISK ASSESSMENT

Nuclear Sector risks are assessed at the facility and sector level as a function of threats, vulnerabilities, and consequences associated with a particular event:

Threat
Natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

Vulnerability
Physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.

Consequence
Effect of an event, incident, or occurrence.

Owners and operators work closely with the NRC and other sector partners to continually assess sector risks and maintain and update risk assessment procedures.

Expanding Safety and Security Assessments to Address Evolving Risks

In the wake of Fukushima, the NRC and the Nuclear Sector are expanding their evaluations of nuclear facility safety and security to consider events beyond the standard design basis accident (DBA): the postulated worst-case accident that a nuclear facility must be designed and built to withstand without loss of systems, structures, or components necessary to ensure public health and safety. Post-Fukushima stress tests of nuclear facilities examined risks from beyond-DBA natural hazards, including earthquakes, tsunamis, severe storms, flooding, tornadoes, volcanic activity, and deliberate attacks. Facilities also were evaluated for their ability to withstand multiple simultaneous events. Examples include the earthquake and tsunami that hit Fukushima. Events involving multiple reactor accidents at a single large nuclear power plant also were evaluated. The Nuclear Sector similarly expanded its risk assessments following the September 11th attacks.

Research to Assess Risks of Aging Infrastructure

As an increasing number of nuclear power plants and other nuclear facilities move into their fifth or sixth decade of operation, partners are working to understand how the resilience of such facilities changes over the lifecycle of materials and systems. NRC and the Nuclear Sector have extensive research programs on aging materials, monitoring, continuous upgrades, and other issues related to the safety and security of facilities over a lifetime that some experts predict could extend to 100 years.

Sector-wide and Cross-sector Risk Assessments

DHS conducts risk assessments for each of the 16 critical infrastructure sectors working with SSAs, State and local authorities, and private sector owners and operators.

DHS Radiological/Nuclear Terrorism Risk Assessment (RNTRA)

The DHS Chemical and Biological Defense Division (CBD) collaborates with the DHS Domestic Nuclear Detection Office (DNDO) and interagency partners to develop and execute the RNTRA. The biennial assessment is based on a rigorous mathematical methodology and uses multiple models to analyze information from the intelligence, law enforcement, scientific, medical, and public health communities. The RNTRA estimates the human casualty and economic consequences of radiological and nuclear terrorism, informing emergency responders, decision-makers, and policy makers regarding resource allocation and countermeasures.[17] The RNTRA supports the Integrated Chemical, Biological, Radiological, and Nuclear Terrorism Risk Assessment mandated in Homeland Security Presidential Directive 18: Medical Countermeasures against Weapons of Mass Destruction.

Implement Risk Management Activities

The NRC and the U.S. nuclear industry work closely together to improve the resilience of all U.S. nuclear facilities by reducing the risk of accidents, incidents, or attacks to individual facilities, and implementing measures to ensure the continued operation or safe shutdown of critical assets and services during an emergency.

Several risk reduction activities may be required by the NRC rules. However, owners and operators also work in a voluntary, collaborative capacity with the NRC and other sector partners to 1) effectively implement both voluntary and regulated state-of-the-art security measures and testing at individual facilities; 2) participate in training, workshops, and programs that improve the knowledge and capabilities of staff; and 3) ensure that new regulations, when developed, represent industry best practices and achievable security measures. This section describes the key risk management activities conducted by Nuclear Sector partners.

Force-on-Force Exercises

Building on lessons learned from the September 11th attacks, NRC strengthened security programs, reevaluated its DBT, and improved Force-on-Force exercises. In November 2004, NRC began implementing its redesigned, full-scale Force-on-Force program. NRC has increased the frequency of its Force-on-Force exercises so that each nuclear power plant site will conduct an NRC-evaluated exercise at least once every three years, and nuclear power plants themselves will conduct annual tactical response security drills in the intervening years. Force-on-Force exercises assess a nuclear plant's physical protection measures to defend against the DBT. The DBT describes an adversary that plant owners must protect against with physical protection systems and response strategies. NRC periodically reassesses the DBT and revises it if necessary. Force-on-Force exercises identify potential gaps and lessons learned that owners and operators use to continually improve their security measures.

Continuous Security Enhancements

The NRC is continuously evaluating and strengthening its overall security program in response to changes in the threat environment, technological advances, and lessons learned. As a result, substantial improvements to nuclear power plant security have been made to secure facilities against terrorism and radiological sabotage, including intensively trained security forces, robust physical barriers, intrusion detection systems, surveillance systems, and plant access controls.

The DOE NNSA provides voluntary security enhancements and specialized training through its Global Threat Reduction Initiative (GTRI) at sites that use Category 1 and 2 radioactive sources. GTRI takes a comprehensive approach to reduce and protect vulnerable nuclear and radiological material that includes 1) converting facilities from highly enriched uranium to low enriched uranium, 2) removing or confirming the disposal of excess materials, and 3) protecting high-priority nuclear and radiological materials from theft. Entities that participate in GTRI programs must first meet all regulatory requirements. Both appropriate facility personnel and local law enforcement agencies are eligible for the GTRI training programs. Since May 2004, GTRI has:[18]

- Accelerated the establishment of a reliable supply of the medical isotope molybdenum-99, produced without highly enriched uranium.
- Removed more than 36,000 disused and unwanted radiological sources from sites across the United States.
- Completed physical protection upgrades at more than 1,700 U.S. and international buildings with high-activity radiological sources.
- Provided Alarm Response Training to more than 3,000 site security personnel, law enforcement officers, and other first responders.

Integrated Planning, Training, and Exercises

The Nuclear Sector is strengthening its incident response capabilities through integrated planning and exercises that include all major stakeholders. Enhanced coordination, planning, and exercises help to improve sector communications, promote consistency, and ensure integration of the National Incident Management System into preparedness plans and incident management.

- NEI offers courses for nuclear industry professionals on emergency preparedness planning and training, radiation protection, and mitigation of specific risks such as fire protection.
- NEI holds frequent workshops for nuclear security professionals to engage in dialogue and learn from industry and NRC experiences in the Force-on-Force program.
- The Silent Thunder exercise series is a collaborative effort between NNSA and the FBI that is aimed at building critical, hands-on experience in responding to a terrorist attack involving radiological materials for Federal, State, and local officials; first responders; and law enforcement.
- The Integrated Response exercise series is a collaborative effort between the FBI, State and local first responders, and nuclear power generation facilities to ensure mutual aid response capabilities inside the protective area at each facility.

Exploring Alternative Medical Technologies to Secure or Replace High-risk Isotopes

Partners continue to explore measures to secure or potentially replace particularly high-risk NRC-licensed radioisotopes used in healthcare and industrial settings. If stolen or otherwise misappropriated, these materials could be used in a radiological dispersal device (RDD) or a radiological exposure device (RED). Nuclear GCC and SCC members are working through a variety of programs and initiatives to ensure that radioactive sources are used only as intended.

Enhanced Transportation Security Measures for GTCC Sources and Materials

Progress has been made in addressing ongoing challenges regarding transportation of sealed sources that exceed commercial disposal activity limits. NRC is revising its guidance on commercial disposal of sealed sources. The private sector is developing new transportation containers to facilitate recovery of lost or abandoned high-activity sources and devices. NRC is working on a final Environmental Impact Statement (EIS) for the disposal of Greater-than-Class-C LLW.

Training and Coordination to Increase Physical Protection of Radioactive Source Materials

- Public education efforts and coordination among Federal, State, local, tribal, and territorial government organizations on radioactive source security have made significant strides. For example, one of seven projects is the Public Education Action Plan developed by the Interagency Public Education Steering Committee for the 2010 Radiation Source Protection and Security Task Force Report. It was completed in 2013 and can serve as a foundation for a guide for communicating with the public following RDD events. This completes a triad of communications guides for radiological and nuclear events: nuclear power plant accidents, improvised nuclear devices, and RDDs.
- The United States is increasing participation in a wide range of international activities that aim to increase the security of radioactive sources in research, healthcare, and industry. At the 2012 (Seoul, South Korea) and 2014 (The Hague, Netherlands) Nuclear Security Summits, radioactive source security received high-level attention. The U.S. sponsored a Joint Statement at the 2014 Summit, signed by 22 other countries, that expresses the signatories' intent to secure all Category 1 sources within their territories by 2016.
  - The United States continues to support IAEA efforts to encourage nations to make a political commitment to work toward following the guidance in the 2004 IAEA Code of Conduct. As of August 2014, 122 nations had signed on, an increase of 22 nations since 2010. The United States participated in organizing IAEA's 2013 *International Conference on the Safety and Security of Radioactive Sources: Maintaining Continuous Control throughout the Lifecycle*, in Abu Dhabi, United Arab Emirates.
  - The United States was instrumental in periodically convening the 10-member ad hoc group of countries that are major suppliers of radioactive sources to continue a dialogue on ways to improve export controls for radioactive sources and develop best practices for repatriation of legacy sources.
- The EPA, in cooperation with a number of industry associations, has developed training materials for demolition contractors and scrap yard workers on identifying and properly handling abandoned or improperly disposed sources.

3.2 Managing Cyber Risks

Nuclear energy facilities use both digital and analog systems to monitor plant processes, operate equipment, and store and retrieve information. Analog systems follow hard-wired instructions; digital computer systems use software to provide instructions. Digital systems, including individual computers and networks, are vulnerable to cyberattacks, which include malicious exploitation and infection by malware, such as viruses, worms, and other types of programming code.

Nuclear energy facilities are designed to shut down safely if necessary, even if there is a breach of cybersecurity. A cyberattack has a low probability of affecting critical systems in a nuclear energy facility or their safety functions. Among other measures, these critical systems are not connected to the Internet or to a facility's internal network. The isolation of critical safety systems minimizes the pathways for a cyberattack. Nuclear energy facilities also are designed to automatically disconnect from the power grid if there is a disturbance that could be caused by a cyberattack.[19] DHS—along with its intelligence community and private sector partners, the NRC, and DOE—has standing working groups that routinely review these safety features.

For more than a decade, the nuclear industry has taken steps to improve its cybersecurity both at an individual facility level and through regulations and programs. In 2002, the Nuclear Energy Institute (NEI) developed the first comprehensive cybersecurity program in the energy sector designed specifically for control system and critical infrastructure security. All nuclear power plants had implemented the system by 2008.

In 2009, **NRC developed its comprehensive cybersecurity regulations.** Each nuclear power plant operator has received NRC approval for a cybersecurity plan that describes how it is implementing its cybersecurity program and a schedule describing steps it has taken to fully implement the program. NRC has reviewed these schedules and regularly inspects nuclear power plant cybersecurity. NRC required each nuclear power plant to:

- Establish a dedicated cybersecurity assessment team under its cybersecurity plan.
- Identify critical systems and critical digital assets that fell within the scope of the NRC requirements.
- Isolate key control systems using either air-gaps or robust hardware-based isolation devices.
- Implement robust controls of portable media and equipment (such as thumb drives, CDs, and laptops), including minimizing the use of devices that are not maintained at the plant, scanning devices for viruses both before and after being connected to plant equipment, and implementing additional security measures when the source of the data or device originates outside the plant.
- Enhance defenses against insider threats by implementing training and insider mitigation programs that include cyber attributes, increasing security screening of individuals who work with digital plant equipment, and increasing cybersecurity training and behavioral observation.

NRC's cybersecurity team includes technology and threat assessment experts who team with other Federal agencies and the nuclear industry to evaluate and help resolve issues that could affect digital systems. This team makes recommendations to other offices within the NRC and is also designing a cybersecurity inspection program for future implementation. All sites will be required to satisfy those inspection requirements.

DHS routinely works with the NRC and private sector partners to identify cyber threats, vulnerabilities, and consequences in the sector. DHS holds **monthly classified cybersecurity briefings** with the Nuclear Sector to share current risk information. In 2015, DHS worked with the sector to complete an internal review of cyber issues, dependencies, and guidance in the Nuclear Sector.

In 2011, the Nuclear Sector helped develop the ***Cross-Sector Roadmap for Cybersecurity of Control Systems***, which provides milestones over a 10-year timeframe to guide voluntary efforts to improve the cybersecurity of control systems that operate critical processes in all critical infrastructure sectors.

The Nuclear Sector developed the ***Roadmap to Enhance Cyber Systems Security in the Nuclear Sector*** in 2012 to provide a vision and framework for mitigating cybersecurity risks to the wide variety of systems critical to commercial nuclear power plant operations. It outlines specific goals, objectives, and time-based milestones for the next 15 years that will adequately protect commercial nuclear power from cyber threats, so that the current functional reliability and resilience of the commercial nuclear power subsector of the Nuclear Sector is maintained despite an evolving threat landscape.

In 2012, the NRC established an internal organization component, the Cyber Security Directorate (CSD), to coordinate and manage agency-wide cybersecurity activities for NRC licensees, including rulemaking, guidance, licensing, policy issues, and oversight. The CSD includes a cyber-assessment team to evaluate whether an identified threat could impact licensed facilities and provides recommendations to the NRC.[20]

The NRC is collaborating with the Federal Energy Regulatory Commission, the North American Electric Reliability Corporation (NERC), and other organizations on cybersecurity. The **NRC has signed a Memorandum of Understanding with NERC to clarify the regulatory roles and responsibilities** of each organization, including inspection protocols and enforcement actions. This MOU ensures a continuity of cybersecurity oversight that extends from the plant itself to the electrical grid as a whole.

The Nuclear Sector is now working with DHS to develop **sector-specific guidance for implementing the National Institute of Standards and Technology (NIST) Cybersecurity Framework**, which provides a voluntary, flexible approach to managing cyber risks. Rather than prescriptive steps, it offers a repeatable framework to assess cybersecurity risk and prioritize cost-effective solutions. The Nuclear Sector is participating in the Critical Infrastructure Cyber Community (C^3) Voluntary Program to promote implementation of the Cybersecurity Framework using the forthcoming guidance.

3.3 Mitigating Disruptions from the Loss of Lifeline Functions

The Nuclear Sector is tightly integrated with the Energy and Water Sectors and dependent on essential services provided by the Transportation Systems and Communications Sectors. Owners and operators develop contingency plans, backup generation supplies, and alternate communications methods and transportation routes as part of their emergency operations and business continuity plans. In particular, owners and operators draw upon lessons learned from cross-sector partners during State and local emergency exercises to form more accurate expectations of lifeline function availability during a major disaster.

Nuclear power plants in particular have emergency diesel generators and batteries onsite that can supply electricity during a loss of offsite power and ensure a safe shutdown. Facilities have approximately seven days of fuel onsite for emergency generators. In a long-term electricity outage, facilities would require a functioning fuel and transportation network to deliver additional fuel supplies, or would safely shut down. Power plants also have emergency water reserves onsite that will enable a safe shutdown during a loss of primary cooling water supplies. During a loss of commercial communication networks, facilities have multiple communication protocols for onsite communication, including radio and paper message systems, as well as backup communication methods to contact the NRC.

In 2014, NEI coordinated the nuclear industry's establishment of two National Response Centers: one in Phoenix, Arizona, and one in Memphis, Tennessee. The nuclear industry began developing the centers after Japan's 2011 Fukushima accident. They hold multiple sets of emergency equipment that can be used to supplement permanent safety equipment at nuclear power plants and other nuclear facilities. The centers can deliver backup equipment and emergency generators to any U.S. nuclear power plant within 24 hours. To develop and operate the two centers, the industry established the Strategic Alliance for FLEX Emergency Response (SAFER).

Facilities that contain radiological isotopes work with local emergency responders to develop incident response plans that ensure the safety and security of radiological materials during the loss of critical lifeline functions. The NNSA offers security training programs for law enforcement to help develop and execute safe and secure emergency response plans.

In 2015, the National Infrastructure Advisory Council released its *Executive Collaboration for the Nation's Strategic Infrastructure* report, which provides recommendations for senior-level, cross-sector engagement to address interdependencies in the Nation's critical infrastructure sectors. Efforts to improve cross-sector collaboration stemming from this report will help the Nuclear Sector better understand, plan for, and mitigate lifeline sector dependencies.

3.4 Research and Development Priorities

Research and development (R&D) is critical in developing new technologies and methods to assess risks and vulnerabilities of Nuclear Sector assets. There are many cross-cutting research and development efforts, not only within the U.S. Department of Homeland Security, but also Federal agencies, academia, and the international arena. Several members of the Nuclear GCC and SCC maintain relevant R&D programs, as do private sector associations, such as EPRI, and international partners, such as the IAEA.

R&D requirements for the Nuclear Sector are identified over the course of frequent interagency coordination through the Nuclear GCC and other interagency and public-private forums. The Nuclear SSA will work with partners to continually collect and prioritize capability requirements that can be supported by technology development. This information may then be used to determine whether current Federal and interagency R&D programs meet requirements or if new programs are needed.

To a large extent, Nuclear Sector partners benefit from the same technology as other critical infrastructure sectors. Common R&D requirements include communications interoperability; personal identity verification and authentication; technical surveillance, monitoring, and detection capabilities; and cybersecurity tools and capabilities. R&D priorities specific to the Nuclear Sector include:

- Modeling, simulation, and analysis products to support security and resilience decision-making in the sector.
- Secure methodologies and assessments to advance state-of-the art reactor consequence analyses, particularly approaches that incorporate offsite health and economic consequences and may be used to support cross-sector comparisons.
- Secure supply-chain analysis for radiological byproduct material (e.g., sealed sources and radioisotopes), considering both security and continuity-of-supply aspects.
- Secure hardware and system to support real-time tracking of individual high-risk radioactive sources to enable timely detection and response to the theft or diversion of such source(s).
- Secure hardware and systems to support surveillance, detection, and monitoring of multiple threats in the owner-controlled area of a commercial nuclear power plant.

Cybersecurity R&D needs will continue to be considered along with non-cyber R&D needs; however, such needs will be identified by the existing Joint Nuclear Cybersecurity Subcouncil and developed in consultation with DHS and other members of the CSCSWG, as appropriate.

These Nuclear Sector R&D priorities contributed to and align with the cross-sector R&D priority areas identified in the 2015 *National Critical Infrastructure Security and Resilience Research and Development Plan*. National R&D priorities include:

- Develop the foundational understanding of critical infrastructure systems and systems dynamics.
- Develop integrated and scalable risk assessment and risk management approaches.
- Develop integrated and proactive capabilities, technologies, and methods to support secure and resilient infrastructure.
- Harness the power of data sciences to create unified, integrated situational awareness and to understand consequences of action.
- Build a crosscutting culture of critical infrastructure security and resilience research and development collaboration.

The Nuclear Sector will work closely with its Federal partners to support implementation of the Nuclear Sector priorities in direct support of National R&D Plan implementation.

3.5 Critical Infrastructure and National Preparedness

Presidential Policy Directive 8: National Preparedness affirmed that national preparedness to major threats is a shared responsibility of all levels of government and the private and nonprofit sectors, and called for a National Preparedness System to help align the efforts of all partners for prevention, protection, mitigation, response, and recovery. Section 3.1 provides an overview of the sector's key approaches to **disaster prevention, protection**, and **risk mitigation**. The sector also extensively prepares for effective sector **response** and **recovery** that supports the resilience of critical sector operations and regional and national resilience as a whole.

When transitioning to incident response and recovery, Nuclear Sector partners rely on robust emergency action plans that define operational security procedures, such as information protection; threat and suspicious incident analysis centers; planned, scaled responses to varying threat levels; and coordination with law enforcement agencies.

NRC Response to Emergency Events

In the event of a serious emergency at a U.S. commercial nuclear power plant or nuclear facility, NRC is prepared to respond immediately. Its headquarters Operations Center is staffed 24 hours a day with specially trained responders who monitor the activities of NRC licensees. They also are available to alert officials if NRC's incident response resources are needed. NRC's incident response policies, procedures, and facilities are regularly tested with drills and exercises. Its response program is evaluated and updated as needed, with the goal of ensuring that NRC is ready to respond at all times.

If a significant incident occurs, the NRC activates its Operations Center in Rockville, Maryland, and one or more of its four regional Incident Response Centers. Specially trained and qualified personnel are alerted to report to duty stations immediately. The NRC incident response program uses a flexible, graduated system to tailor its response to the significance of an event. For example, depending on the type of event and its safety or security significance, NRC might move from "normal" response mode to "monitoring mode." This puts key regional staff into position to ensure the licensee is handling the event correctly. This also puts other responders on notice they may be called into the Operations Center or Incident Response Centers.

If necessary, NRC could then enter "activation mode," in which the necessary safety, security, and support specialists report to the Operations Center. The final emergency response mode is called "expanded activation." It is entered when an incident's severity or uncertainty warrants sending a team of NRC experts directly to the site of the event.

When the NRC goes into activation mode, skilled and trained responders assemble. Some responders will work directly with the nuclear power plant or facility operators to independently assess the severity of the event, and some will evaluate licensee protective action recommendations. Other responders will liaison with the media, State and local governments, other Federal agencies, Congress and the White House, and the international nuclear community. Although the nuclear power plant or facility operator is responsible for returning the site to a safe condition, the NRC Chairman has the authority to intervene. He or she can direct the licensee's onsite response if necessary.

The NRC tests itself many times each year with drills and exercises that mimic safety and/or security incidents. In addition to full-scale exercises, the Operations Center and Incident Response Centers are occasionally activated for small incidents or potential emergencies.

National Response Centers for Nuclear Power Plants

As part of the nuclear energy industry's response to the Fukushima Daiichi accident, an industry alliance established two National Response Centers that store five sets of backup equipment that can be delivered to any U.S. nuclear power plant within 24 hours. The Strategic Alliance for FLEX Emergency Response (SAFER) operates the response centers through a $400 million investment by the industry over the 40-year life of the program. The centers house portable backup generators, high-pressure and low-pressure pumps, diesel fuel transfer pumps, diesel fuel tanks, diesel-powered light towers, water treatment, and other equipment that can help maintain public health and safety in the face of an extreme event.[21]

Emergency Medical Response

Radiological Emergency Assistance Center/Training Site (REAC/TS), Oak Ridge, Tennessee, under Oak Ridge Associated Universities, continues to work to strengthen medical responses to radiation emergencies. REAC/TS staff members are available 24 hours a day/7 days a week to deploy and provide emergency medical consultation for incidents involving radiation anywhere in the world. REAC/TS provides direct support for the National Nuclear Security Administration's Office of Emergency Response and the Federal Radiological Monitoring and Assessment Center (FRMAC). Adding to its depth of response

and consultation capabilities, REAC/TS is uniquely qualified to teach medical personnel, health physicists, first responders, and occupational health professionals about radiation emergency medical response. REAC/TS also operates a cytogenetic biodosimetry laboratory where chromosome aberration analysis is used for ionizing radiation dose assessment. REAC/TS supports the international community as a World Health Organization (WHO) Collaborating Center of the Radiation Emergency Medical Preparedness and Assistance Network (REMPAN) and as a member of the International Atomic Energy Agency's (IAEA) Response Assistance Network (RANET) for radiation accident response.

Licensee Response

NRC regulations require licensees to have plans for responding to incidents, mitigating their severity, and protecting against radiological releases. NRC reviews and approves these plans and regularly assesses their adequacy and effectiveness through exercises.

If a significant incident occurs, licensees must take immediate actions to ensure safety and security, provide timely notifications to NRC and State and local government authorities, and make recommendations on how to protect the public from potential consequences.

Based on NRC regulations, licensees classify incidents according to the plant conditions and the level of risk to the public. Nuclear power plants, for example, use four emergency classifications:

- **Notification of Unusual Event**—Events are either ongoing or have occurred that indicate a potential decline in the level of plant safety. No release of radioactive material requiring offsite response or monitoring is expected.
- **Alert**—Events are in process or have occurred that involve an actual or potentially substantial decline in the level of plant safety. However, any release of radioactive material is expected to be well below the EPA's protective action guidelines.
- **Site Area Emergency**—Events are occurring or have occurred that involve an actual or potential major failure of the plant's ability to protect the public. Any releases of radioactive material are not expected to exceed the EPA guidelines except near the site boundary.
- **General Emergency**—Events are in progress that involve actual or imminent severe damage or melting of the radioactive fuel in the reactor core. There is a potential for radioactive releases exceeding EPA guidelines beyond the immediate site area.

State and Local Government Responses

State governments, and in some locations local and/or tribal governments, develop and implement emergency plans for NRC-licensed facilities. Although the licensee is responsible for what occurs onsite, State and local governments are responsible for protecting life, property, and the environment offsite.

Through drills and exercises, State and local governments work closely with FEMA and, when appropriate, the NRC. The goal is to ensure that their plans and procedures will protect their community's health and safety.

During an emergency, NRC communicates directly with State and local governments to share information. The NRC may also offer technical advice and assistance if requested.

Federal Response

The NRC works within the National Response Framework to respond to events. The framework guides the Nation in response to complex events of national significance that may involve a variety of agencies and hazards. Under this framework, NRC retains its independent authority and ability to respond to emergencies that involve NRC-licensed facilities or materials. NRC coordinates the overall Federal technical response to an incident that involves one of its licensees.

NRC may ask for support from the Department of Homeland Security (DHS). In addition, DHS may lead and manage the overall Federal response to an event, according to Homeland Security Presidential Directive 5. In this case, NRC would provide technical expertise and help share information among the various organizations and licensees.

Nuclear Power Plants as Resources to Critical Infrastructure in Major Emergencies

Because they are extensively hardened against natural and manmade disasters, nuclear power plants often can continue to operate through hurricanes and other major natural disasters. Because they can keep operating when other power generators cannot, nuclear power plants may be able to provide electricity services during disasters and provide blackstart capabilities to other electricity generators.

CHAPTER ENDNOTES

17. Office of Science and Technology (S&T), U.S. Department of Homeland Security (DHS), "DHS Science and Technology Directorate: Radiological/Nuclear Terrorism Assessment," Fact Sheet, (DHS: March 8, 2012).
18. National Nuclear Security Administration, "GTRI: Reducing Nuclear Threats," last updated May 29, 2014, http://nnsa.energy.gov/mediaroom/factsheets/reducingthreats.
19. Nuclear Energy Institute, "Policy Briefs: Cyber Security for Nuclear Power Plants," April 2015, http://www.nei.org/Master-Document-Folder/Backgrounders/Policy-Briefs/Cyber-Security-Strictly-Regulated-by-NRC;-No-Addit.
20. U.S. Nuclear Regulatory Commission, Office of Nuclear Security and Incident Response, *Protecting Our Nation: A Report of the U.S. Nuclear Regulatory Commission*, (Washington, D.C.: NRC, October 2013).
21. Nuclear Energy Institute, "SAFER: Regional Response Center Facts," fact sheet (NEI, May 22, 2014), http://www.nei.org/CorporateSite/media/filefolder/Backgrounders/Fact-Sheets/Regional-Response-Center-Fact-Sheet.pdf?ext=.pdf; U.S. Nuclear Regulatory Commission, "Watching Response Centers Put Trucks on the Road," August 18, 2014, http://public-blog.nrc-gateway.gov/tag/safer/.

4 VISION, GOALS, AND PRIORITIES

An effective Nuclear Sector partnership is instrumental in achieving the sector vision shared by asset owners, government and community partners, and regulators. The Nuclear Sector GCC and SCC collectively developed five joint goals for sector security and resilience and nine priorities it will pursue over the next four years. These goals and priorities directly support the Nuclear Sector risk management framework and approaches detailed in Chapter 3, and they directly contribute to the Joint National Priorities and the NIPP 2013 Calls to Action, as shown in Appendix B.

NUCLEAR SECTOR VISION

The Nuclear Sector will support national security, public health and safety, and economic stability by enhancing, where necessary and reasonably achievable, its existing high level of readiness to promote the security and resilience of the Nuclear Sector in an all-hazards environment, and to lead by example to improve the Nation's overall critical infrastructure readiness.

Table 1. Nuclear Sector Goals and Priorities

Nuclear Sector Goals	Nuclear Sector Priorities	
1 Establish robust collaboration and communication and promote continuous learning among Nuclear Sector partners and cross-sector stakeholders.	PRIORITY A	Promote voluntary sector and cross-sector coordination through the Nuclear SCC and GCC and foster partnerships with the international community to promote a global culture of Nuclear Sector security and resilience.
	PRIORITY B	Improve Federal mechanisms to deliver timely and relevant risk information and actionable alerts to Nuclear Sector partners while ensuring the protection of classified and Safeguards Information.
	PRIORITY C	Increase the public's awareness of sector security measures, potential consequences, and proper actions following a release of radioactive material, including the liabilities of a lost or stolen source.
2 Continuously identify and assess sector-specific threats, vulnerabilities, and consequences to enable a risk-informed approach to security and resilience enhancements.	PRIORITY D	Identify, characterize, and communicate Nuclear Sector physical, cyber, and human risks and update critical asset identification as risks evolve.
3 Coordinate with sector partners to develop programs and measures that cost-effectively reduce physical and cyber risks from all-hazard incidents impacting Nuclear Sector assets.	PRIORITY E	Improve cybersecurity tools and capabilities to secure Nuclear Sector cyber assets, systems, and networks and to ensure the resilience of the functions they support.
	PRIORITY F	Improve the security, tracking, detection, and disposal of nuclear and radioactive material to prevent its misuse and minimize its accidental introduction into the public domain.
	PRIORITY G	Support permanent risk reduction by promoting and examining opportunities to transition from radioactive source technologies to non-isotopic or lower-activity radioactive source technologies.

Nuclear Sector Goals		Nuclear Sector Priorities
4	Support advance planning and risk mitigation that enables coordinated response and rapid recovery to ensure safe and resilient operation of critical Nuclear Sector services.	PRIORITY H — Increase nuclear asset owner awareness of and coordination with State, local, tribal, and territorial radiation control resources and first responders to promote preparedness, response, and recovery capacity.
5	Promote continuous learning and adaptation among global Nuclear Sector and cross-sector partners during exercises, incidents, and planning.	PRIORITY I — Promote voluntary exercises that engage the full spectrum of nuclear sector security and emergency response stakeholders to improve preparedness and incorporate lessons learned into training and response and recovery planning.

4.1 Nuclear Sector Activities

Nuclear Sector partners in the public and private sectors collaboratively developed a set of 15 activities that they can conduct on a voluntary basis to effectively implement this SSP and meaningfully contribute to the sector goals and priorities. While risk management in the Nuclear Sector is substantially regulated by the NRC, the SSP activities presented here reflect only the voluntary activities that the Nuclear SCC and GCC will participate in or support to reduce risk beyond what is accomplished by regulation alone. The Nuclear SCC and GCC may pursue the following activities under either joint or individual council efforts over the next one to four years. While the Sector-Specific Plans are updated every four years, the Nuclear Sector partnership may update its activities more frequently to reflect evolving risk, changing resource allocations, and progress or completion.

Sector partners are operating in resource-limited environments, and the ability to achieve the identified activities will depend largely on future resource availability, funding allocations, and sector-wide prioritization processes. Resource limitations may not allow for completion of all identified activities. Rather than develop priorities and activities based solely on currently available funding, the sector identified the top activities it believes will make a significant contribution to national security and resilience. Sector partners can use this activity list to prioritize resources as they become available. The Nuclear SCC and GCC will meet annually to prioritize and build on the SSP activities. During this time, the councils will further develop a list of discrete, detailed tasks to pursue over the coming year, considering timing, available resources, and feasibility.

Table 2. Nuclear Sector Activities Mapped to Sector Priorities

Map to Priority		Sector Activities
A	1	Continue to increase interaction with public and other stakeholders through social media and other sources to improve understanding of regulatory processes, safeguards, activities, and emergency response plans.
B E	2	Request that Federal partners sponsor additional security clearances for the nuclear industry, particularly for cybersecurity experts.
B D	3	Expedite the release of unclassified tear lines to nuclear asset owners and operators and engage private sector experts with Federal intelligence collection and analysis to improve the relevance of Nuclear Sector information sharing.
B F	4	Work with other Federal agencies to develop reciprocity agreements to accept Department of Justice background investigations and NRC clearances that enable individuals to access critical areas of nuclear power facilities and provide security.

Map to Priority		Sector Activities
A D	5	Provide Nuclear SCC and GCC (including SLTT partner) expertise and recommendations to multiple Federal interagency working groups on nuclear and radiological security and review planning documents, including the Nuclear/Radiological Incident Annex to the National Response Framework.
A	6	Broaden Nuclear SCC membership to include individuals with relevant expertise, such as independent spent fuel storage installation.
A	7	Work with sector partners to improve information sharing and best practices through facility tours, meetings, and other opportunities for engagement.
D E F	8	Conduct remaining site visits under NNSA's Radiological Security Program—for public and commercial facilities Category 1 and Category 2 licensees who request them—to identify voluntary security enhancements that can further increase the protection of radioactive sources and material.
D F	9	Support the continued national implementation of the NNSA Radiological Security Program's cesium chloride (CsCl) In-Device Delay kits, already installed at more than 200 sites, to impede a potential adversary's access to radiological materials.
A F	10	Work with national and international partners to continue widely implementing the National Source Tracking System, a secure, Web-based national database to enhance the accountability of radioactive sources and improve information sharing with government agencies, as applicable.
F	11	Reduce the number of disused radioactive source stores in U.S. facilities and support source disposal cost-sharing with Category 1 and Category 2 licensees by coordinating efforts among asset owners and Federal, regional, and local radiation control stakeholders.
G	12	Work with asset owners and end users within the Radioactive Isotopes Working Group to identify and study alternative, non-radioactive technologies to replace Category 1 and 2 technologies, while ensuring uninterrupted access to these resources for end users who comply with relevant safety and security requirements. Continue to seek end-user feedback on source application and usefulness of Category 1 and 2 technologies and replacement alternative technologies.
H I	13	Conduct voluntary Integrated Response exercises to coordinate event response of onsite security, operations, and emergency response personnel with offsite responders, such as State and local emergency management, fire and emergency medical responders, law enforcement, and asset owners in interdependent sectors. Work with SLTT partners to identify resources and personnel to support exercises and planning.
A H I	14	Continue to work with Federal and SLTT partners to expand implementation of RadResponder capabilities among SLTT radiological emergency preparedness organizations to improve environmental data sharing capabilities. The RadResponder network includes more than 2,900 responders.
G F	15	Implement the recommendations of the Radiation Source Protection and Security Task Force reports established by the Energy Policy Act of 2005, as applicable.

5 MEASURING EFFECTIVENESS

Owners and operators use a variety of indicators to measure the effectiveness and continuous improvement of their security and resilience risk management processes at the facility level. Measuring improvements in security and resilience at the sector level is far more difficult. Where possible, Nuclear Sector partners attempt to measure how their voluntary partnership activities contribute to risk reduction and enhanced resilience across the sector.

As the Sector-Specific Agency, the U.S. Department of Homeland Security has the primary responsibility for measuring and reporting progress toward sector activities using relevant metrics. An established performance metrics system designed to track the progress of sector activities is used to ensure accurate and consistent measurement.

The following table aligns Nuclear Sector activities with a set of performance metrics that the Sector-Specific Agency may use to measure and report progress, where possible. The metrics not only measure the completion of an activity—using output measures, such as the number of products developed or partners engaged—but also aim to measure the outcomes of these activities—particularly how effective they are in achieving progress toward sector goals.

Within the voluntary sector partnership, often the best available outcome measure is to track intent to act based on the information, tools, or guidance received through sector activities. The Sector-Specific Agency measures this intent to act using a survey—during or following each engagement or activity—that asks three things:

- Was the information received current and relevant?
- Will the information inform decision-making?
- Will participants share the information within their organization?

Survey results indicate the effectiveness of each activity in equipping participants with the information, tools, guidance, and processes to take actions that ultimately reduce or better manage sector risk.

The Sector-Specific Agency will report sector progress through the National Annual Report and the quadrennial Sector-Specific Plan updates. The following list is not exhaustive of all possible ways to measure effectiveness, and sector asset owners may voluntarily measure and report additional information on sector progress during the National Annual Reporting process.

Table 3. Nuclear Sector Activities and Expected Metrics

	Nuclear Sector Activities	Expected Metrics
1	Continue to increase interaction with public and other stakeholders through social media and other sources to improve understanding of regulatory processes, safeguards, activities, and emergency response plans.	• Information products developed and their level of distribution • Relevancy and intended use of information received
2	Request that Federal partners sponsor additional security clearances for the nuclear industry, particularly for cybersecurity experts.	• Number of clearances granted • Relevancy and intended use of information received
3	Expedite the release of unclassified tear lines to nuclear asset owners and operators and engage private sector experts with Federal intelligence collection and analysis to improve the relevance of Nuclear Sector information sharing.	• Products developed and their level of distribution • Relevancy and intended use of information received

	Nuclear Sector Activities	Expected Metrics
4	Work with other Federal agencies to develop reciprocity agreements to accept Department of Justice background investigations and NRC clearances that enable individuals to access critical areas of nuclear power facilities and provide security.	• Status of developing reciprocity agreements • Relevancy and intended use of information received
5	Provide Nuclear SCC and GCC (including SLTT partner) expertise and recommendations to multiple Federal interagency working groups on nuclear and radiological security and review planning documents, including the Nuclear/ Radiological Incident Annex to the National Response Framework.	• Meetings or working groups organized or coordinated to provide expertise and recommendations • Products developed and their level of distribution • Relevancy and intended use of information received
6	Broaden Nuclear SCC membership to include individuals with relevant expertise, such as independent spent fuel storage installation.	• Sector Coordinating Council membership • Sector Coordinating Council meetings and level of member participation • Relevancy and intended use of information received
7	Work with sector partners to improve information sharing and best practices through facility tours, meetings, and other opportunities for engagement.	• Facility tours, meetings, and engagements organized or coordinated and level of participation • Relevancy and intended use of information received
8	Conduct remaining site visits under NNSA's Radiological Security Program—particularly for public and commercial Category 1 and Category 2 licensees who request them—to identify voluntary security enhancements that can further increase the protection of radioactive sources and material.	• Products and/or voluntary security enhancements developed • Relevancy and intended use of information received
9	Support the continued national implementation of the NNSA Radiological Security Program's cesium chloride (CsCl) In-Device Delay kits, already installed at more than 200 sites, to impede a potential adversary's access to radiological materials.	• Information products developed and their level of distribution • Workshops and/or trainings held and the level of participation • Relevancy and intended use of information received
10	Work with national and international partners to continue widely implementing the National Source Tracking System, a secure, Web-based national database to enhance the accountability of radioactive sources and improve information sharing with government agencies, as applicable.	• Status of implementing the National Source Tracking System • Relevancy and intended use of information received

	Nuclear Sector Activities	Expected Metrics
11	Reduce the number of disused radioactive source stores in U.S. facilities and support source disposal cost-sharing with Category 1 and Category 2 licensees by coordinating efforts among asset owners and Federal, regional, and local radiation control stakeholders.	• Meetings and working groups organized or coordinated with asset owners and Federal, regional, and local radiation control stakeholders • Products developed and their level of distribution • Relevancy and intended use of information received
12	Work with asset owners and end users within the Radioactive Isotopes Working Group to identify and study alternative, non-radioactive technologies to replace Category 1 and 2 technologies, while ensuring uninterrupted access to these resources for end users who comply with relevant safety and security requirements. Continue to seek end-user feedback on source application and usefulness of Category 1 and 2 technologies and replacement alternative technologies.	• Meetings and working groups organized or coordinated with asset owners and end users and level of participation • Products developed and their level of distribution
13	Conduct voluntary Integrated Response exercises to coordinate event response of onsite security, operations, and emergency response personnel with offsite responders, such as State and local emergency management, fire and emergency medical responders, law enforcement, and asset owners in interdependent sectors. Work with SLTT partners to identify resources and personnel to support exercises and planning.	• Number of exercises organized or coordinated and the level of participation • Relevancy and intended use of information received
14	Continue to work with Federal and SLTT partners to expand implementation of RadResponder capabilities among SLTT radiological emergency preparedness organizations to improve environmental data sharing capabilities.	• Status of implementation of Rad Responder capabilities • Meeting and working groups organized or coordinated and level of participation • Products developed and their level of distribution • Relevancy of information recipients receive and how they intend to use it
15	Implement the recommendations of the Radiation Source Protection and Security Task Force reports established by the Energy Policy Act of 2005, as applicable.	• Status of implementing recommendations • Any products developed and their level of distribution • Relevancy and intended use of information received

APPENDIX A
ACRONYMS AND ABBREVIATIONS

AC	alternating current
ACI	American Concrete Institute
AEA	Atomic Energy Act
AEC	Atomic Energy Commission
ANS	American Nuclear Society
ANSI	American National Standards Institute
ASCE	American Society of Civil Engineers
ASME	American Society of Mechanical Engineers
ASNT	American Society for Non-Destructive Testing
BWR	boiling water reactors
C³	Critical Infrastructure Cyber Community
CBD	Chemical and Biological Defense Division
CBP	Customs and Border Protection
CFDI	Critical Foreign Dependencies Initiative
CFR	Code of Federal Regulations
CIPAC	Critical Infrastructure Partnership Advisory Council
CoC	Certificate of Compliance
CNS	Center for Nonproliferation Studies
CRCPD	Conference of Radiation Control Program Directors
CsCl	cesium chloride
CSD	NRC Cyber Security Directorate
CSCSWG	Cross-Sector Cyber Security Working Group
DBA	design basis accident
DBT	design basis threat
DHS	U.S. Department of Homeland Security
DNDO	Domestic Nuclear Detection Office
DOD	U.S. Department of Defense
DOE	U.S. Department of Energy
DOJ	U.S. Department of Justice
DTRA	Defense Threat Reduction Agency
EIS	Environmental Impact Statement
EO	Executive Order
EPRI	Electrical Power Research Institute
ERDA	Energy Research and Development Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FRMAC	Federal Radiological Monitoring and Assessment Center
FRPCC	Federal Radiological Preparedness Coordinating Committee
GCC	Government Coordinating Council
GDP	gaseous diffusion plants
GTCC	Greater-than-Class-C
GTRI	Global Threat Reduction Initiative
HEU	highly enriched uranium
HHS	U.S. Department of Health and Human Services
HLW	high-level waste
HPS	Health Physics Society
HSPD	Homeland Security Presidential Directive
IAEA	International Atomic Energy Agency
ICSJWG	Industrial Control Systems Joint Working Group
IEEE	Institute of Electrical and Electronics Engineers
INMM	Institute of Nuclear Materials Management
INPO	Institute of Nuclear Power Operators
IP	DHS Office of Infrastructure Protection
ITDB	Incident and Trafficking Database
ISSEIS	Integrated Safety and Security Enforcement and Interdiction System
LEU	low enriched uranium
LLC	Limited Liability Corporation
LLW	low-level waste
LVS	Licensed Verification System
Mo-99	molybdenum-99
MOU	memorandum of understanding
MW	megawatts
NEI	Nuclear Energy Institute
NGCC-RTR	Nuclear GCC Research and Test Reactor Subcouncil
NIPP 2013	*National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience*
NIST	National Institute of Standards and Technology
NNSA	National Nuclear Security Administration
NORM	naturally occurring radioactive material
NRC	Nuclear Regulatory Commission
NSCC-R	Nuclear SCC Radioisotopes Subcouncil
NSCC-RTR	Nuclear SCC Research and Test Reactor Subcouncil
NSTS	National Source Tracking System
OAS	Organization of Agreement States

OCIA	DHS Office of Cyber and Infrastructure Analysis
OMB	Office of Management and Budget
PPD	Presidential Policy Directive
PRA	probabilistic risk assessment
PWR	pressurized water reactors
R&D	research and development
RadSTraM	Radiological Source Tracking and Monitoring System
RANET	IAEA's Response Assistance Network
RDD	radiological dispersal device
REAC/TS	Radiological Emergency Assistance Center/Training Site
RED	radiological exposure device
REMPAN	WHO Collaborating Center of the Radiation Emergency Medical Preparedness and Assistance Network
REP	Radiological Emergency Preparedness
RERP	Radiological Emergency Response Plan
RTTR	research, training and test reactors
SAFER	Strategic Alliance for FLEX Emergency Response
SCC	Sector Coordinating Council
SLTT	State, local, tribal, and territorial
SLTTGCC	State, Local, Tribal, and Territorial Government Coordinating Council
SNM	Special Nuclear Material
SOPD	Sector Outreach and Programs Division
SSA	Sector-Specific Agency
SSNM	Strategic special nuclear material
SSP	Sector-Specific Plan
SWG	Security Working Group
TE-NORM	Technologically-enhanced Naturally Occurring Radioactive Material
TRTR	National Organization of Test, Research and Training Reactors
TSA	Transportation Security Administration
UF6	uranium hexafluoride
U.S.	United States
U.S.C.	United States Code
USCG	U.S. Coast Guard
USNORTHCOM	U.S. Northern Command
WANO	Atlanta Center of the World Association of Nuclear Operators
WBL	Web-based Licensing System
WHO	World Health Organization
WINS	World Institute for Nuclear Security
WMD	weapon of mass destruction

APPENDIX B
ALIGNMENT WITH THE NIPP 2013

This appendix illustrates the alignment of Nuclear Sector priorities (objectives) with the NIPP 2013 national goals and Joint National Priorities, and the ways in which sector activities contribute to the NIPP 2013 Calls to Action.

Table B-1. Nuclear Sector Priorities Aligned with Joint National Priorities and NIPP Goals

Nuclear Sector Priorities	Joint National Priorities					NIPP Goals
	Strengthen Management of Cyber and Physical Risks to Critical Infrastructure	Build Capabilities and Coordination for Enhanced Incident Response and Recovery	Strengthen Collaboration Across Sectors, Jurisdictions, and Disciplines	Enhance Effectiveness in Resilience Decision-making	Share Information to Improve Prevention, Protection, Mitigation, Response, and Recovery Activities	
A Promote voluntary sector and cross-sector coordination through the Nuclear SCC and GCC and foster partnerships with the international community to promote a global culture of Nuclear Sector security and resilience.		PRIORITY A	PRIORITY A	PRIORITY A	PRIORITY A	Share information across the critical infrastructure community to build awareness and enable risk-informed decision-making.
B Improve Federal mechanisms to deliver timely and relevant risk information and actionable alerts to Nuclear Sector partners while ensuring the protection of classified and Safeguards Information.		PRIORITY B		PRIORITY B	PRIORITY B	
C Increase the public's awareness of sector security measures, potential consequences, and proper actions following a release of radioactive material, including the liabilities of a lost or stolen source.			PRIORITY C	PRIORITY C	PRIORITY C	
D Identify, characterize, and communicate Nuclear Sector physical, cyber, and human risks and update critical asset identification as risks evolve.	PRIORITY D	PRIORITY D		PRIORITY D		Assess and analyze risks to critical infrastructure to inform risk management activities.

Nuclear Sector Priorities		Joint National Priorities					NIPP Goals
		Strengthen Management of Cyber and Physical Risks to Critical Infrastructure	Build Capabilities and Coordination for Enhanced Incident Response and Recovery	Strengthen Collaboration Across Sectors, Jurisdictions, and Disciplines	Enhance Effectiveness in Resilience Decision-making	Share Information to Improve Prevention, Protection, Mitigation, Response, and Recovery Activities	
E	Improve cybersecurity tools and capabilities to secure Nuclear Sector cyber assets, systems, and networks and to ensure the resilience of the functions they support.	PRIORITY E	PRIORITY E		PRIORITY E		Secure critical infrastructure against physical, cyber, and human threats through sustainable risk reduction efforts, while considering costs and benefits.
F	Improve the security, tracking, detection, and disposal of nuclear and radioactive material to prevent its misuse and minimize its accidental introduction into the public domain.	PRIORITY F	PRIORITY F	PRIORITY F	PRIORITY F		
G	Support permanent risk reduction by promoting the transition from radioactive source technologies to non-isotopic or lower-activity radioactive source technologies.	PRIORITY G	PRIORITY G		PRIORITY G		
H	Increase nuclear asset owner awareness of and coordination with State, local, tribal, and territorial radiation control resources and first responders to promote preparedness, response, and recovery capacity.				PRIORITY H	PRIORITY H	Enhance critical infrastructure resilience by minimizing consequences and employing effective response and recovery.
I	Promote voluntary exercises that engage the full spectrum of Nuclear Sector security and emergency response stakeholders to improve preparedness and incorporate lessons learned into training and response and recovery planning.		PRIORITY I	PRIORITY I	PRIORITY I	PRIORITY I	Promote learning and adaptation during and after incidents and exercises.

Table B-2.Contribution of Nuclear Sector Activities to the NIPP 2013 Calls to Action

	Nuclear Sector Contribution or Aligned Activity	NIPP 2013 Calls to Action											
		#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	#11	#12
1	Continue to increase interaction with public and other stakeholders through social media and other sources to improve understanding of regulatory processes, safeguards, activities, and emergency response plans.			X									
2	Request that Federal partners sponsor additional security clearances for the nuclear industry, particularly for cybersecurity experts.			X		X							
3	Expedite the release of unclassified tear lines to nuclear asset owners and operators and engage private sector experts with Federal intelligence collection and analysis to improve the relevance of Nuclear Sector information sharing.					X							
4	Work with other Federal agencies to develop reciprocity agreements to accept Department of Justice background investigations and NRC clearances that enable individuals to access critical areas of nuclear power facilities and provide security.					X							
5	Provide Nuclear SCC and GCC (including SLTT partner) expertise and recommendations to multiple Federal interagency working groups on nuclear and radiological security and review planning documents, including the Nuclear/ Radiological Incident Annex to the National Response Framework.					X					X		
6	Broaden Nuclear SCC membership to include individuals with relevant expertise, such as independent spent fuel storage installation.					X							
7	Work with sector partners to improve information sharing and best practices through facility tours, meetings, and other opportunities for engagement.					X							X
8	Conduct remaining site visits under NNSA's Radiological Security Program—particularly for public and commercial Category 1 and Category 2 licensees who request them—to identify voluntary security enhancements that can further increase the protection of radioactive sources and material.						X						
9	Support the continued national implementation of the NNSA Radiological Security Program's cesium chloride (CsCl) In-Device Delay kits, already installed at more than 200 sites, to impede a potential adversary's access to radiological materials.							X	X				
10	Work with national and international partners to continue widely implementing the National Source Tracking System, a secure, Web-based national database to enhance the accountability of radioactive sources and improve information sharing with government agencies, as applicable.						X						
11	Reduce the number of disused radioactive source stores in U.S. facilities and support source disposal cost-sharing with Category 1 and Category 2 licensees by coordinating efforts among asset owners and Federal, regional, and local radiation control stakeholders.						X						
12	Work with asset owners and end users within the Radioactive Isotopes Working Group to identify and study alternative, non-radioactive technologies to replace Category 1 and 2 technologies, while ensuring uninterrupted access to these resources for end users who comply with relevant safety and security requirements. Continue to seek end-user feedback on source application and usefulness of Category 1 and 2 technologies and replacement alternative technologies.										X		
13	Conduct voluntary Integrated Response exercises to coordinate event response of onsite security, operations, and emergency response personnel with offsite responders, such as State and local emergency management, fire and emergency medical responders, law enforcement, and asset owners in interdependent sectors. Work with SLTT partners to identify resources and personnel to support exercises and planning.			X			X						

	Nuclear Sector Contribution or Aligned Activity	NIPP 2013 Calls to Action											
		#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	#11	#12
14	Continue to work with Federal and SLTT partners to expand implementation of RadResponder capabilities among SLTT radiological emergency preparedness organizations to improve environmental data sharing capabilities.							X	X				
15	Implement the recommendations of the Radiation Source Protection and Security Task Force reports established by the Energy Policy Act of 2005, as applicable.										X		
	Nuclear Sector goals and priorities were developed in alignment with the 2014 Joint National Priorities in support of Call to Action #1.	X											
	Development of the 2015 Nuclear Sector-Specific Plan meets Call to Action #2.		X										
	The Nuclear Sector supports Call to Action #10 by working with its Federal partners to implement the National Critical Infrastructure Security and Resilience Research and Development Plan.										X		
	The measurement approach outlined in Chapter 5: Measuring Effectiveness will enable the Nuclear Sector to evaluate and report on the progress of partnership efforts in support of Call to Action #11.											X	

NIPP 2013 Calls to Action

Call to Action #1: Set National Focus through Jointly Developed Priorities

Call to Action #2: Determine Collective Actions through Joint Planning Efforts

Call to Action #3: Empower Local and Regional Partnerships to Build Capacity Nationally

Call to Action #4: Leverage Incentives to Advance Security and Resilience

Call to Action #5: Enable Risk-Informed Decision-making through Enhanced Situational Awareness

Call to Action #6: Analyze Infrastructure Dependencies, Interdependencies, and Associated Cascading Effects

Call to Action #7: Identify, Assess, and Respond to Unanticipated Infrastructure Cascading Effects During and Following Incidents

Call to Action #8: Promote Infrastructure, Community, and Regional Recovery Following Incidents

Call to Action #9: Strengthen Coordinated Development and Delivery of Technical Assistance, Training, and Education

Call to Action #10: Improve Critical Infrastructure Security and Resilience by Advancing Research and Development Solutions

Call to Action #11: Evaluate Progress toward the Achievement of Goals

Call to Action #12: Learn and Adapt During and After Exercises and Incidents

APPENDIX C
NUCLEAR SECTOR TAXONOMY AND CATEGORIES

Taxonomy of Nuclear Sector Assets and Facilities

Nuclear Power Plants

- Boiling water reactors (BWR)
- Pressurized water reactors (PWR)

Research, Training, and Test Reactors

- Government research and test reactors
- University research and training reactors
- Private research and test reactors

Decommissioned Nuclear Facilities

- Deactivated reactors
- Other deactivated nuclear facilities

Fuel Cycle Facilities

- Uranium mining or in situ uranium leaching
- Uranium ore milling or leachate processing
- Uranium conversion facilities
- Uranium enrichment facilities

Fuel Fabrication Facilities

- Category I (special nuclear materials) facilities
- Category II (special nuclear materials—moderate strategic significance) facilities
- Category III (special nuclear materials—low strategic significance) facilities

Nuclear Materials Transport

- Low-hazard radioactive materials transport
- High-hazard radioactive materials transport

Radioactive Materials

- Medical facilities with radioactive materials
- Research facilities using radioactive materials
- Irradiation facilities
- Industrial facilities with nuclear materials

Radioactive Source Production and Distribution Facilities

- Radioactive device manufacturers
- Radioactive source producers
- Radioactive source importers
- Radioactive source manufacturers

Used Fuel and Radioactive Waste

- Low-level radioactive waste processing and storage facilities
- Sites managing accumulations of naturally occurring radioactive materials (NORM)

Spent Nuclear Fuel Processing and Storage Facilities

- Spent nuclear fuel wet storage facilities
- Spent nuclear fuel dry storage facilities
- Transuranic waste processing and storage facilities
- High-level radioactive waste storage and disposal facilities
- Mixed waste processing

Categories of Fuel Cycle Facilities

Category I Fuel Cycle Facilities

Licensed to receive, possess, use, and store a Category I quantity of strategic special nuclear material (SSNM). SSNM consists of uranium-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope), uranium-233, or plutonium.

- Category I quantity of SSNM is 5,000 grams or more in any combination computed by the formula: (grams contained U-235) + 2.5(grams U-233 + grams plutonium).

Category II Fuel Cycle Facilities

Licensed to receive, possess, use, and store special nuclear material (SNM) of moderate strategic significance. Category II quantity of material is either:

- Less than Category I quantity of SSNM, but more than 1,000 grams of uranium-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope), or more than 500 grams of uranium-233 or plutonium, or the combination of more than 1,000 grams computed by the formula: (grams contained U-235) + 2(grams U-233 + grams plutonium).
- 10,000 grams or more of uranium-235 (contained in uranium enriched to 10 percent or more, but less than 20 percent in the U-235 isotope).

Category III Fuel Cycle Facilities

Licensed to receive, possess, use, and store SNM of low strategic significance. Category III quantity of material is any one of the following:

- Less than an amount of SNM of moderate strategic significance, but more than 15 grams of uranium-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope), or 15 grams of uranium-233 or plutonium, or the combination of 15 grams when computed by the formula: (grams contained U-235) + (grams plutonium) + (grams U-233).
- Less than 10,000 grams but more than 1,000 grams of uranium-235 (contained in uranium enriched to 10 percent or more, but less than 20 percent in the U-235 isotope).
- 10,000 grams or more of uranium-235 (contained in uranium enriched above natural, but less than 10 percent in the U-235 isotope).

Category III Fuel Enrichment Facilities

Gaseous Diffusion Plants (GDPs)

- One operating GDP and one in cold shutdown in the United States, both operated by the United States Enrichment Corporation, which was created as a government corporation under the Energy Act of 1992 and privatized by legislation in 1996.

- Certified to receive, possess, use, and store source material (or natural uranium, less than 5.5 percent enriched) and SNM.
- Manufacture feed materials—enriched uranium hexafluoride (UF6)—for commercial fuel fabricator facilities.

Gas Centrifuge Uranium Enrichment Facilities

- One facility in the United States (not operational).
- Certified to receive, possess, use, and store source material (or natural uranium, up to 5 percent enriched) and SNM.
- Manufactures feed materials—enriched UF6—for commercial fuel fabricator facilities.

Uranium Conversion Facilities (UF6 Production Facilities)

Licensed to receive, possess, use, and store source material (natural uranium). Manufacture feed materials in the form of UF6 for commercial fuel enrichment facilities. Currently, there is one UF6 production facility licensed by the NRC in the United States.

APPENDIX D
NUCLEAR SECTOR AUTHORITIES

Nuclear Sector security and resilience requires considerable cooperation and coordination among diverse entities in the public and private sectors. Numerous legal authorities govern this work. These legal authorities and their responsibilities for sector assets are summarized in this appendix.

Department of Homeland Security

The authority of the Department of Homeland Security (DHS) is derived from the **Homeland Security Act**, Public Law 107-296, 116 Stat. 2135 (2002), and a number of Homeland Security Presidential Directives (HSPDs).

On December 17, 2003, the President issued **HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection**, which "establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attack." The Secretary of DHS, in accordance with paragraph 29 of HSPD-7, will continue to work with the NRC and DOE to ensure protection of Nuclear Sector assets. In accordance with paragraph 25 of HSPD-7, DHS and the SSA will collaborate with appropriate private sector entities and continue to encourage development of information-sharing and analysis mechanisms. In addition, DHS and the SSA will collaborate with the private sector and continue to support mechanisms for sector coordination, such as:

- Identifying, prioritizing, and coordinating the security and resilience of critical infrastructure.
- Facilitating information sharing about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices.

Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21) replaces HSPD-7 and directs the Executive Branch to develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time, understand the cascading consequences of infrastructure failures, evaluate and mature the public-private partnership, update the National Infrastructure Protection Plan, and develop a comprehensive research and development plan.

Many different HSPDs are also relevant to critical infrastructure security and resilience, including, but not limited to:

- HSPD-3: Homeland Security Advisory System
- HSPD-5: Management of Domestic Incidents
- HSPD-8: National Preparedness
- HSPD-9: Defense of the United States Agriculture and Food
- HSPD-10: Biodefense for the 21st Century
- HSPD-19: Combating Terrorist Use of Explosives in the United States
- HSPD-20: National Continuity Policy
- HSPD-22: Domestic Chemical Defense

Domestic Nuclear Detection Office

On April 15, 2005, the President issued **HSPD-14/National Security Presidential Directive 43: Domestic Nuclear Detection Office** (DNDO). This directive established DNDO within DHS to:

- Serve as the primary entity in the U.S. Government to further develop, acquire, and support deployment of an enhanced domestic system to detect and report attempts to import, possess, store, transport, develop, or use an unauthorized nuclear explosive device, fissile material, or radioactive material in the United States, and to improve that system over time.
- Enhance and coordinate nuclear detection efforts of Federal, State, territorial, local, and tribal governments and the private sector to ensure a managed, coordinated response.

- Establish, with approval of the Secretary of Homeland Security and in coordination with the Attorney General and Secretaries of Defense and Energy, additional protocols and procedures for use within the United States to ensure that detection of unauthorized nuclear explosive devices, fissile material, or radioactive material is promptly reported to the Attorney General; the Secretaries of Defense, Homeland Security, and Energy; and other appropriate officials or their respective designees for appropriate action by law enforcement, military, emergency response, or other authorities.
- Develop, with approval of the Secretary of Homeland Security and in coordination with the Attorney General and the Secretaries of State, Defense, and Energy, an enhanced global nuclear detection architecture with several implementation considerations: 1) DNDO will be responsible for implementation of the domestic portion of the global architecture; 2) the Secretary of Defense will retain responsibility for implementation of Department of Defense (DOD) requirements within and outside the United States; and 3) the Secretaries of State, Defense, and Energy will maintain their respective responsibilities for policy guidance and implementation of the portion of the global architecture outside the United States, which will be implemented consistent with relevant laws and international arrangements.
- Conduct, support, coordinate, and encourage an aggressive, expedited, evolutionary, and transformational program of R&D efforts to advance the science of nuclear and radiological detection.
- Support and enhance the effective sharing and use of appropriate information generated by the Intelligence Community, counterterrorism community, law enforcement agencies, other government agencies, and foreign governments, as well as provide appropriate information to those entities.
- Further enhance and maintain continuous awareness by analyzing information from all DNDO mission-related detection systems.

Federal Emergency Management Agency

On December 7, 1979, the President directed the Federal Emergency Management Agency (FEMA) to take lead responsibility for all offsite nuclear planning and response. FEMA's activities are conducted according to **Energy Management and Assistance**, 44 Code of Federal Regulations (CFR), parts 350, 351, and 352. These regulations are a key element in the Radiological Emergency Preparedness (REP) Program, established following the Three Mile Island Nuclear Power Station accident in March 1979.

FEMA rule 44 CFR, part 350 establishes the policies and procedures for the REP Program's initial and continued approval of State, local, and tribal governments' radiological emergency planning and preparedness for commercial nuclear power plants. This approval is contingent partly on State and local government participation in joint exercises with licensees. The REP Program's responsibilities in radiological emergency planning for fixed nuclear facilities include:

- Leading offsite emergency planning and reviewing and evaluating Radiological Emergency Response Plans (RERPs) and procedures developed by State and local governments.
- Determining whether such plans and procedures can be implemented on the basis of observation and evaluation of exercises of the plans and procedures conducted by State and local governments.
- Responding to requests by the Nuclear Regulatory Commission (NRC) according to the memorandum of understanding (MOU) between it and FEMA dated June 17, 1993 (44 CFR, part 354, Appendix A, September 14, 1993).
- Coordinating the activities of Federal agencies with responsibilities in the radiological emergency planning process through the Federal Radiological Preparedness Coordinating Committee (FRPCC) and Regional Assistance Committee.

Department of Transportation

The Federal **Hazardous Materials Transportation Act**, 49 U.S.C. 5101 et seq., and the **Pipeline Safety Statute**, 49 U.S.C. 60101 et seq., give the Secretary of Transportation the regulatory and enforcement authority to enhance the safe transportation of hazardous materials by all modes and hazardous liquids and natural gas by pipeline. The Secretary also has the authority to marshal transportation in a defined area to aid in national defense and homeland security through the **Defense Production Act of 1950**, 50 U.S.C. App. 2071, and the **Robert T. Stafford Disaster Relief and Emergency Assistance Act**, 42 U.S.C. 5121 et seq. In allocating or prioritizing civil transportation resources, the Secretary, with

appropriate funding from one of three agencies (DOD, the Department of Energy (DOE), or DHS), has extensive authority, in all modes, to organize transportation during an emergency. Also, the **Homeland Security Act of 2002** amended the hazardous materials transportation law to include security, so the mandate now reads that the Secretary of Transportation can "prescribe regulations for the safe transportation, including security, of hazardous materials in intrastate, interstate, and foreign commerce."

Department of Energy

The **Atomic Energy Act** (AEA), as amended, 42 U.S.C. 2011 et seq., is the primary source of DOE's authority for its nuclear science, technology, and R&D activities, as well as its nuclear weapons programs. The AEA also authorizes DOE's production, ownership, and use of special nuclear, source, and byproduct material. DOE regulations on nuclear activities are set forth in 10 CFR, parts 820, 830, and 835.

Principal DOE Statutory Authorities

- **Atomic Energy Act of 1954, as amended**: Under the AEA, DOE is broadly authorized to conduct R&D in military and civilian applications of atomic energy and nuclear reactor production for the U.S. Navy; conduct the Nation's nuclear weapons programs; provide for related storage, transportation, and disposal of hazardous and radioactive waste; and regulate nuclear safety. The AEA was amended most recently by the Energy Policy Act of 2005.
- **Energy Reorganization Act of 1974**: Sections 104 and 201 of the act abolished the Atomic Energy Commission (AEC) created by the AEA and transferred its functions to the NRC and the Administrator of the Energy Research and Development Administration (ERDA). Commercial licensing and related regulatory functions of the AEC were transferred to the NRC, and ERDA assumed AEC responsibility for activities that include nuclear energy R&D and operation of nuclear weapons programs.
- **Department of Energy Organization Act**: In 1977, ERDA was terminated and its functions transferred to the Secretary of Energy by sections 301 and 703 of the act.

Other DOE Statutory Authorities

- **Nuclear Waste Policy Act of 1982, as amended**: DOE is responsible for site characterization, construction, and operation of a geological repository for disposal of the Nation's high-level radioactive waste and spent nuclear fuel. DOE is also responsible for transportation of high-level radioactive waste and spent nuclear fuel to the repository. Section 180 of the act requires DOE to transport the waste and spent fuel in NRC-certified packages and according to NRC regulations regarding advance notification to State and local governments.
- **National Nuclear Security Administration (NNSA) Act of 2000**: The NNSA was established by the National Defense Authorization Act for Fiscal Year 2000. The NNSA is a semi-autonomous agency within DOE. Its mission includes activities related to national security, nonproliferation, and safety and reliability of nuclear weapons.
- **Energy Policy Act of 2005 (EPAct)**: Among other activities, EPAct directed DOE to undertake several initiatives regarding nuclear energy R&D. Section 641 of the act provides for establishment of the Next-Generation Nuclear Plant Project, consisting of R&D and, ultimately, operation of a prototype nuclear reactor that could potentially generate electricity and produce hydrogen. Section 952 also directs DOE to conduct nuclear energy research programs, including the Generation IV Nuclear Energy Systems Initiative to develop an overall technology plan to support necessary R&D for promising technologies for new commercial reactors. Section 651(d) requires establishment of an interagency task force, with DOE membership, to report to the President and Congress on the security of radiation sources in the United States from potential threats and to develop recommendations for possible regulatory and legislative changes related to protection and security of sources.

Nuclear Regulatory Commission

The AEA, as amended, is the primary source of the NRC's authority to regulate radioactive material and civilian nuclear activities. NRC regulations are set forth in 10 CFR, parts 0–199.

The NRC and its licensees share a common responsibility to protect public health and safety. Supporting Federal regulations and the NRC regulatory program are important elements in protecting the public. NRC licensees, however, have day-to-day responsibility for ensuring safe use of nuclear material.

Principal NRC Statutory Authorities

- **Atomic Energy Act of 1954, as amended**: Under the AEA, the NRC has broad authority to regulate (by regulation, licensing, or order) possession, transfer, and use of source, byproduct, and Special Nuclear Material (SNM) to protect public health and safety and to provide for the common defense and security. Under AEA Section 147, 42 U.S.C. 2167, the NRC also has authority to designate information as Safeguards Information to prevent its unauthorized disclosure.

- **Energy Reorganization Act of 1974**: This act abolished the AEC and moved its regulatory function to the NRC, establishing the NRC as an independent regulator of certain nuclear material and facilities. The act also created what eventually became DOE. DOE addresses military uses of AEA materials, as well as nuclear energy research. Unless specifically authorized by legislation, the NRC does not regulate DOE activities, which include promotion of nuclear energy and development of nuclear material for military uses.

Other NRC Statutory Authorities

- **Nuclear Non-Proliferation Act of 1978**: This act (in combination with the AEA) gives the NRC the authority to license export and import of nuclear material and equipment to ensure these items are used for peaceful purposes. For all nuclear exports, the NRC must find that export will not be "inimical to the common defense and security." No commercial export license for nuclear facilities, source material, or SNM may be issued by the NRC unless the U.S. Government and country of export have an agreement for meeting the requirements of AEA Section 123, 42 U.S.C. 10143.

- **Uranium Mill Tailings Radiation Control Act of 1978**: This act regulates uranium mill tailings and any remediation that might be associated with the mill sites.

- **Nuclear Waste Policy Act of 1982, Nuclear Waste Policy Act Amendments of 1987, and EPAct of 1992**: These acts, in combination, set forth requirements for development and licensing of Yucca Mountain, a proposed high-level radioactive waste repository being developed by DOE. In contrast to the NRC's legislatively mandated authority to regulate disposal, the NRC's ability to regulate transportation to the repository is specifically limited by the Nuclear Waste Policy Act, as amended, to the certification of transportation packages and pre-notification of shipments.

- **Diplomatic Security and Anti-Terrorism Act of 1986**: This act requires the Secretaries of Defense, State, and Energy and the NRC to review the adequacy of physical security standards currently applicable to SNM shipment and storage outside the United States, which is subject to U.S. prior-consent rights, with special attention to protection against terrorist acts. The act also requires these officials and the NRC to report to specified congressional committees on the results of such review. The act amends the AEA to require that each licensee or applicant to operate a utilization facility (e.g., a nuclear power reactor) fingerprint each individual who is permitted unescorted access to the facility or is permitted access to certain Safeguards Information. The act provides that all fingerprints are submitted to the Attorney General for identification and a criminal records check, with all costs paid by the licensee or applicant.

- **Solar, Wind, Waste, and Geothermal Power Production Incentives Act of 1990**: This act amended the AEA to require licensing of uranium enrichment facilities, other than existing gaseous diffusion plants (GDPs).

- **EPAct of 2005**: As part of the EPAct, the NRC is required to conduct security evaluations, including Force-on-Force exercises, not less than once every three years at licensed commercial power reactor facilities. The design basis threat (DBT) will include rulemaking and public comment. The NRC must assign a Federal security coordinator employed by the NRC in each region, and it is required to promulgate regulations establishing a mandatory tracking system for radiation sources in the United States. The EPAct establishes a Radiation Source Protection and Security Task Force to evaluate and provide recommendations to Congress and the President on the security of radiation sources in the United States from potential threats, and expands the scope of fingerprinting and criminal history checks at licensee facilities. In coordination with the Department of Justice (DOJ), the EPAct allows for use of a broader class of weapons to protect NRC-licensed or NRC-certified facilities or materials; expands criminal sanctions for sabotage of nuclear facilities, fuel, or materials; expands provisions for unlawful trespass with dangerous weapons, explosives, and other dangerous instruments; and requires the NRC to consult with DHS regarding the proposed location of new utilization facilities.

Agreement States

Section 274b of the AEA allows the NRC to relinquish its regulatory authority over certain materials and certain activities in a State if agreed-upon conditions are met. Agreement States issue licenses and regulate approximately 18,000 materials licensees, only a small fraction of which possess risk-significant radioactive material. Currently, 37 States have section 274b agreements; one State has submitted a Letter of Intent (LOI) for becoming an Agreement State.

Under the 274b agreements, the NRC interacts frequently with the States on licensing, inspection, enforcement, incident response, training, and rulemaking. The NRC provides technical assistance, primarily to Agreement States, and sponsors conferences and special workshops on topics of interest when needed. Agreement States report significant incidents involving materials to the NRC Headquarters Operations Center. More detailed event descriptions are later entered into an events database. The NRC maintains Office of Management and Budget (OMB) clearances for the needed information collections.

Federal Bureau of Investigation

In addition to the FBI's overarching terrorism response authorities as outlined in various National Security, Presidential Policy, and Homeland Security Presidential Directives, the following statutes apply specifically to its enforcement of statutes aimed at preventing criminal and terrorist activity involving nuclear and radioactive material:

- **Atomic Energy Act,** 42 U.S.C. 2011-2284
- **Prohibited Transactions Involving Nuclear Materials**, 18 U.S.C. 831
- **Participation in Nuclear and Weapon of Mass Destruction (WMD) Threats to the United States**, 18 U.S.C. 832
- **WMD Statute**, 18 U.S.C. 2332a

As also stated in the National Response Framework, the Attorney General, generally acting through the FBI, has lead responsibility for criminal investigations of terrorist acts or threats and for coordinating other members of the law enforcement community to detect, prevent, preempt, investigate, and disrupt attacks against the United States, including those involving nuclear and radioactive material.

Homeland Security