



DEFEND TODAY, SECURE TOMORROW

INTRODUCTION TO THE NUCLEAR SECTOR RISK MANAGEMENT AGENCY

Nuclear Reactors, Materials, and Waste Sector (or Nuclear Sector) assets are generally owned and operated by the private sector, and are the most highly regulated and heavily guarded of all civilian infrastructure. The Nuclear Regulatory Commission (NRC) regulates the civilian use of nuclear and radiological 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. 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. With collaboration from sector partners, the Cybersecurity and Infrastructure Security Agency (CISA), which serves as the Nuclear Sector Risk Management Agency (SRMA), maintains and implements a Sector-Specific Plan (SSP), which defines sector goals and objectives guiding the voluntary efforts of sector partners to collectively support the security and resilience posture of our Nation’s critical nuclear facilities and materials.

NUCLEAR SECTOR COLLABORATION, RESOURCES, AND TRAINING

CISA offers many resources to help owners and operators manage risk, improve security, and aid in the implementation and execution of protective and response measures across the Nuclear Sector. This fact sheet lists a sampling of sector collaboration mechanisms, resources, and training materials. Unless otherwise noted below, additional information can be found on the CISA website at cisa.gov/nuclear-reactors-materials-and-waste-sector.

Collaboration

Nuclear Government Council (GCC), Sector Coordinating Council (SCC), Subcouncils, and Working Groups convene regularly; share information; and develop tools, guidelines, and products. These groups work closely to plan, implement, and execute sector-wide resilience and security programs within the Nuclear Sector.

CISA holds quarterly **classified cybersecurity briefings** with the Nuclear Sector to share current risk information and identify cyber threats, vulnerabilities, and consequences within the Sector. Additional briefings may be held as needed.

Critical Infrastructure Threat Information Sharing Framework is a guide for critical infrastructure owners and operators, as well as other critical infrastructure security and resilience stakeholders, that describes how threat information is shared between federal government and owners and operators. Learn more at dhs.gov/publication/ci-threat-info-sharing-framework.

Resources

Nuclear Sector Cybersecurity Framework Implementation Guidance provides a common language that Nuclear Sector owners and operators can use to assess and manage their cybersecurity risks, and use the National Institute of Standards and Technology (NIST) voluntary Framework for Improving Critical Infrastructure Cybersecurity.

Business Continuity Planning Suite helps businesses create, improve, or update their business continuity plans with scalable, easy-to-use software. Learn more at ready.gov/business-continuity-planning-suite.

The DHS Hometown Security initiative focuses on four steps—Connect, Plan, Train, Report—and provides tools and resources to help businesses improve proactive safety and security. Learn more at cisa.gov/hometown-security.

Training

Critical Infrastructure Training includes web-based security awareness training opportunities on the topics of workplace security, active shooter preparedness, insider threat mitigation, surveillance activities, and theft and diversion.

Counter-Improvised Explosive Device (IED) Training & Awareness course options include bombing prevention workshops, soft target awareness, and surveillance detection.

Security seminars and exercises for nuclear industry stakeholders feature subject matter experts and a variety of topics (e.g., active shooter, vehicle-borne improvised explosive devices, and cybersecurity).

SECTOR PROFILE

The U.S. civilian Nuclear Reactors, Materials, and Waste Sector includes the Nation's 96 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.



25 private companies and public power utilities own and operate all 96 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 Reactors, Materials, and Waste Sector does **not** include U.S. Department of Defense (DOD) or U.S. Department of Energy (DOE) defense-related nuclear facilities or nuclear materials.

CRITICAL INFRASTRUCTURE SECURITY CONSIDERATIONS

- **Natural Disasters and Extreme Weather:** Major storms, earthquakes, and tsunamis can severely damage critical operating and emergency equipment. These threats are taken into consideration during the construction and maintenance of each facility.
- **Aging Infrastructure and Workforce:** The initial operating license of U.S. nuclear power plants is 40 years, and NRC has renewed the original operating licenses for 73 U.S. nuclear power units for an additional 20 years. In addition to aging infrastructure, approximately 38 percent of the U.S. nuclear industry workforce will be eligible to retire within five years. Attracting new talent has become a demanding task as the industry faces a shortage of qualified workers and increased competition for college graduates.
- **Deliberate Attacks and Terrorism:** Nuclear power plants continue to evaluate and protect facilities against the threat of targeted large-scale terrorist attacks, which, if successful, could lead to contamination within the surrounding community, widespread power disruptions, or injuries and damage. Emerging concerns include small, unmanned aerial systems (UAS) and other types of remotely operated vehicles that could be used for surveillance or to launch small-scale attacks.
- **Cyberattacks:** The Nuclear Reactors, Materials, and Waste 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, UAS, and other items; state-sponsored industrial espionage; Internet-based financial tampering; embedded malware; and supply chain attacks.

FOR MORE INFORMATION ON THE NUCLEAR SECTOR

Contact the Nuclear Sector Management Team at NuclearSector@cisa.dhs.gov or learn more at cisa.gov/nuclear-reactors-materials-and-waste-sector. View the Nuclear Sector-Specific Plan at: cisa.gov/publication/nipp-ssp-nuclear-2015.