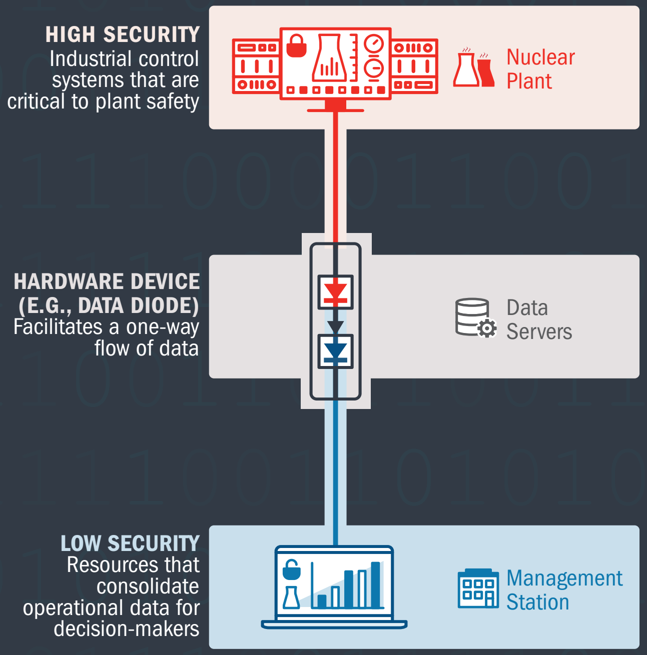
CYBERSECURITY IN THE NUCLEAR SECTOR

Nuclear power reactors produce 20% of our nation's electricity. Ensuring the safety and security of these facilities is a top priority. Since the September 11, 2001 terrorist attacks, the Nuclear industry has pursued comprehensive cybersecurity efforts that incorporate robust cybersecurity policies, procedures, and practices to protect these vital components of our critical infrastructure.

Data Flow and Security Mechanisms

FOR NUCLEAR PLANTS

Nuclear Power Plants are protected from cyberattacks using a defense-in-depth concept in which security controls are layered throughout the network. One part of this approach is a hardware device that only allows data to flow from high-security areas to low-security areas.



HIGH SECURITY
Industrial control systems that are critical to plant safety

Nuclear Plant

HARDWARE DEVICE (E.G., DATA DIODE)
Facilitates a one-way flow of data

Data Servers

LOW SECURITY
Resources that consolidate operational data for decision-makers

Management Station

CISA CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

NSCC NUCLEAR SECTOR COORDINATING COUNCIL

ELEMENTS OF A

Defense-in-Depth Approach

CYBERSECURITY READINESS

Critical assets that perform safety, security, and emergency preparedness functions at nuclear power plants, as well as critical components needed to safely operate and shutdown the reactor, are protected from cyberattacks.

The Nuclear industry adapts to threats by learning about the latest tactics and tools of cyberattackers through participation in information-sharing activities with the U.S. government, including classified threat briefings.

INSIDER THREAT MITIGATION

Individuals who work with digital plant equipment are subject to background checks, extensive security screening, cybersecurity training, and behavioral observation.

PORTABLE MEDIA CONTROLS

Strict controls over the use of thumb drives, laptops, and other portable media are maintained. These devices are regularly scanned for malware.

CYBER INCIDENT RESPONSE

Personnel at nuclear power plants are trained to identify, contain, and eradicate a threat.

In the unlikely event of a successful cyberattack, a nuclear reactor may be powered down, maintained in a safe shutdown condition, and disconnected from the power grid.

SUPPLY CHAIN RISK MANAGEMENT

Supply chain risks are minimized by being aware of evolving cyber security threats, only purchasing assets from approved vendors with a trusted distribution path, and testing assets prior to installation to ensure they operate securely.

ONGOING MONITORING AND OVERSIGHT

Utilities perform ongoing monitoring of their assets to ensure the equipment is functioning properly, to identify potential vulnerabilities and cyberattacks.

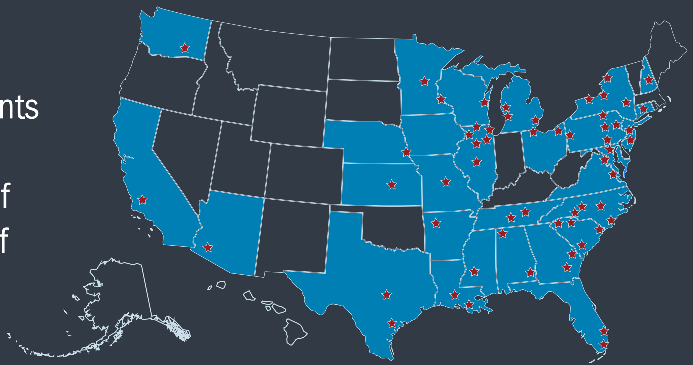
The Nuclear Regulatory Commission (NRC) performs oversight of their program with a resident inspector at each U.S. nuclear plant who reviews all issues that the plant has identified and forwards cybersecurity issues to cybersecurity specialists in the region. In addition, the cybersecurity programs are periodically evaluated by an NRC inspection team to ensure they have been properly implemented.

Sector Relationships

Department, Agency, or Organization	Information Sharing	Regulations & Standards	Research & Development
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY Serves as the Sector Risk Management Agency for the Nuclear Sector, allowing the Nuclear industry and government to discuss cyber-related issues collaboratively; shares classified and unclassified intelligence related to emerging cyber risks and vulnerabilities.	✓	✓	
U.S. NUCLEAR REGULATORY COMMISSION Develops and implements policies and programs related to regulatory oversight and licensing reviews for cybersecurity of NRC-licensed facilities, including commercial power reactors.	✓	✓	
NUCLEAR ENERGY INSTITUTE Develops cybersecurity guidance for the Nuclear industry.	✓	✓	
NUCLEAR SECTOR COORDINATING COUNCIL Facilitates the gathering of Nuclear industry representatives to address cybersecurity-related issues with government support.	✓		
DEPARTMENT OF ENERGY Establishes cybersecurity best practices and provides funding for cybersecurity initiatives relevant to the Nuclear Sector.		✓	
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER Shares information on all electricity-related matters, including cybersecurity issues affecting the Nuclear Sector.	✓		
FEDERAL ENERGY REGULATORY COMMISSION/NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION Develops critical infrastructure and cybersecurity standards.		✓	
ELECTRIC POWER RESEARCH INSTITUTE AND NATIONAL LABS Conducts research and development in support of enhanced security at nuclear facilities.			✓

Nuclear Power Plants in the United States

96 commercial nuclear reactors at **58** power plants in **29** states accounting for approximately **20%** of the Nation's generation of electricity.

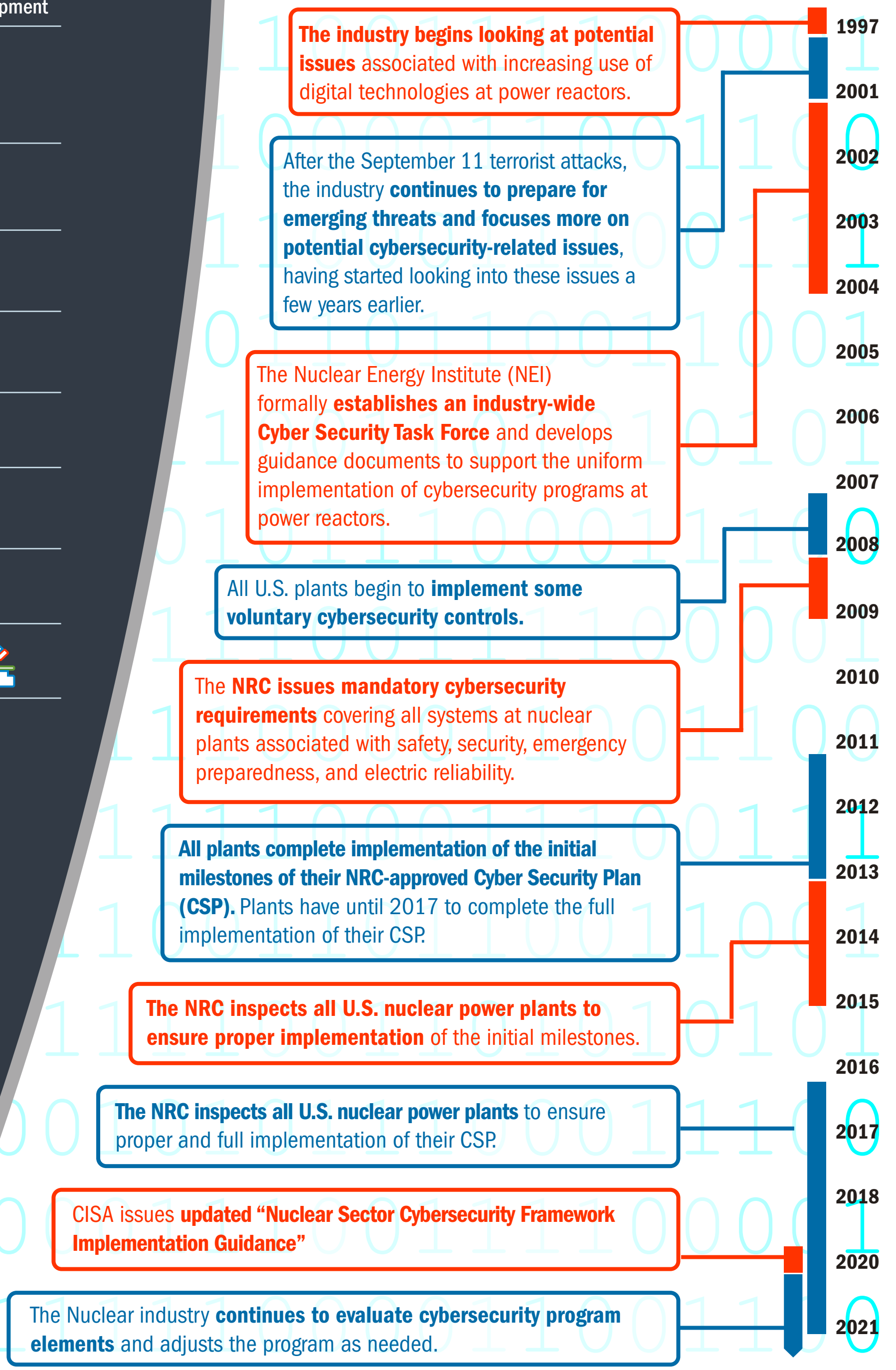


Additional Resources

For more information, please visit cisa.gov/nuclear-reactors-materials-and-waste-sector or us-cert.cisa.gov or email NuclearSector@cisa.dhs.gov.

THE NUCLEAR INDUSTRY'S

Evolving Approach to Cybersecurity



The industry begins looking at potential issues associated with increasing use of digital technologies at power reactors.

After the September 11 terrorist attacks, the industry **continues to prepare for emerging threats and focuses more on potential cybersecurity-related issues**, having started looking into these issues a few years earlier.

The Nuclear Energy Institute (NEI) formally **establishes an industry-wide Cyber Security Task Force** and develops guidance documents to support the uniform implementation of cybersecurity programs at power reactors.

All U.S. plants begin to **implement some voluntary cybersecurity controls.**

The **NRC issues mandatory cybersecurity requirements** covering all systems at nuclear plants associated with safety, security, emergency preparedness, and electric reliability.

All plants complete implementation of the initial milestones of their NRC-approved Cyber Security Plan (CSP). Plants have until 2017 to complete the full implementation of their CSP.

The NRC inspects all U.S. nuclear power plants to ensure proper implementation of the initial milestones.

The NRC inspects all U.S. nuclear power plants to ensure proper and full implementation of their CSP.

CISA issues **updated "Nuclear Sector Cybersecurity Framework Implementation Guidance"**

The Nuclear industry **continues to evaluate cybersecurity program elements** and adjusts the program as needed.