BACKGROUNDER
Office of Public Affairs
301.415.8200
www.nrc.gov ■ opa.resource@nrc.gov

Cyber Security

Nuclear power facilities use digital and analog systems to monitor, operate, control and protect their plants. Digital assets critical to plant systems for performing safety and security functions are isolated from the external networks, including the Internet. This separation provides protection from many cyber threats. Even so, all power reactor licensees must implement a cyber security plan under the NRC's cyber security regulations.

Cyber Security Requirements

Each nuclear power plant's cyber security program protects its digital computer and communication systems and networks against cyber attacks, including systems and networks associated with:

- Safety-related functions and secondary functions considered "important-to-safety;"
- Security functions;
- Emergency preparedness functions, including offsite communications; and,
- Support systems and equipment important to safety and security.

A licensee first submits a plan describing how the cyber security program meets the NRC's requirements, including any features or challenges specific to the facility. If the plan meets the requirements, the NRC approves it and issues a Safety Evaluation Report. The NRC reviews and assesses the licensee's cyber security program as part of the NRC's inspection program.

In January 2010, the NRC published Regulatory Guide, RG 5.71. It provided guidance to licensees and license applicants on an acceptable way to meet the cyber security requirements. The guidance includes "best practices" from such organizations as the International Society of Automation, the Institute of Electrical and Electronics Engineers, the National Institute of Standards and Technology, and the Department of Homeland Security. The Nuclear Energy Institute also prepared guidance, deemed by the NRC as acceptable

for use by licensees, on how to protect critical digital assets. All operating power reactor licensees have developed cyber security plans that the NRC reviewed and approved in 2010. The NRC conducts inspections to ensure that operating power reactor licensees are implementing the cyber security programs at their facilities as described in their NRC-accepted cyber security plans.

NRC's Cyber Security Branch

In June 2013, the NRC centralized oversight of the regulatory agency's activities related to cyber security. Today, within the Office of Nuclear Security and Incident Response, the Cyber Security Branch is responsible for planning, coordinating, and managing all agency activities related to cyber security for NRC licensees and applicants. This includes all rulemaking, guidance, licensing, policy issues and oversight related to cyber security requirements.

Cyber security is an element of decommissioning activities for nuclear facilities. Cyber security rulemaking is in progress for fuel cycle facilities, using the lessons learned from power reactor cyber security program implementations. Currently there are no cyber security requirements for Independent Spent Fuel Storage Installations, and research and test reactors. The NRC is considering the need for cyber security requirements for non-power production or utilization facilities and materials licensees.

The NRC's Cyber Assessment Team responds to cyber events at licensed facilities and reviews licensees' actions. It coordinates with other federal agencies and the industry to assess cyber threats and assist in the event of a cyber attack or credible threat to a licensee. Specifically, the team routinely shares information with the Department of Homeland Security's National Cybersecurity and Communications Integration Center and the Federal Energy Regulatory Commission.

The NRC works on cyber security issues with other regulators and organizations, including FERC and the North American Electric Reliability Corporation, whose mission is to ensure the reliability of the North American power grid. In 2010, the NRC signed a Memorandum of Understanding with NERC to clarify the roles and responsibilities of each organization, including inspection protocols and enforcement actions.

Additionally, the NRC participates with other federal regulators and Executive branch agencies on the Cyber Security Forum for Independent and Executive Branch Regulators. Established in 2014, the forum brings together regulators to share best practices and lessons learned in cyber security protection for critical infrastructure.

March 2019