U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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. "Critical digital assets" that interconnect plant systems performing safety, security, and emergency preparedness functions are isolated from 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.[1]

Cyber Security Requirements

For over a decade, the NRC addressed cyber threats and improved programs and oversight for nuclear power plants to protect critical digital assets. Initial requirements were imposed by Orders issued after the September 2001 terrorist attacks. NRC's cyber security rule was finalized in March 2009, covering power reactor licensees and applicants for new reactor licenses. The regulation incorporated measures imposed by the earlier Orders and lessons learned while implementing them.

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 plan then becomes part of the facility's operating license. 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.[2] 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, and the National Institute of Standards and Technology, and the Department of Homeland Security. The Nuclear Energy Institute also prepared guidance, endorsed by the NRC, on how to protect critical digital assets.

The NRC is also considering the need for similar cyber security requirements for fuel cycle and spent fuel storage facilities, non-power reactors, decommissioned nuclear facilities, and materials licensees.

NRC's Cyber Security Directorate

The NRC established a Cyber Security Directorate in June 2013 to centralize the agency's oversight of this important area. The directorate is responsible for planning, coordinating, and managing all agency activities related to cyber security for NRC licensees. This includes all rulemaking, guidance, licensing, policy issues and oversight related to cyber security requirements.

The NRC's Cyber Assessment Team, which is part of the directorate, 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, Industrial Control Systems Cyber Emergency Response Team, the U.S. Computer Emergency Readiness Team programs, and the Federal Energy Regulatory Commission (FERC).

The NRC works on cyber security issues with other regulators and organizations, including FERC and the North American Electric Reliability Corporation (NERC), 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.

The NRC also participates with other government regulators on the Cyber Security Forum for Independent and Executive Branch Regulators, formed in autumn 2014. The NRC's chairman serves as chair of the forum.

December 2014

[1] 10 CFR 73.54

[2] Regulatory Guide 5.71: Cyber Security Programs for Nuclear Facilities.