U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Backgrounder
Office of Public Affairs
Telephone: 301/415-8200   E-mail: opa@nrc.gov

Cyber Security

Background

Nuclear facilities use digital and analog systems to monitor and operate equipment, and to obtain and store vital information. Analog systems do their job by following “hard-wired” instructions, while digital computer-based systems follow instructions (software) stored in memory. In addition, many plant computer systems are now linked to digital networks that extend across the plant, performing safety, security and emergency preparedness functions. Protecting these critical digital assets and the information they contain from sabotage or malicious use is called cyber security. All power reactor facilities licensed by the NRC must have a cyber security program.

Cyber Security Requirements After 9/11

Shortly after the terrorist attacks of Sept. 11, 2001, the NRC ordered its nuclear power plant licensees to enhance their overall security. The order included specific requirements for addressing certain cyber security threats and vulnerabilities. The order contains sensitive information and is not available to the public,

A year later, the NRC issued another order that, for the first time, added cyber attacks to the adversary threat types the plants must be able to defend against. This order also contains sensitive information and is not available to the public.

In October 2004, the NRC again addressed cyber security concerns by publishing a self-assessment tool for use by nuclear power plants. In 2005, the NRC also endorsed a program developed by the Nuclear Energy Institute to help nuclear power reactor licensees establish and maintain cyber security programs at their facilities. Additional cyber security guidance was published in January 2006 and March 2007. It included specifics for designing, developing and implementing protective measures for digital instrumentation and controls used in nuclear safety-related applications.

In March 2009, the NRC issued a new cyber security rule. This new section of the NRC Code of Federal Regulations, “Protection of Digital Computer and Communications Systems and Networks” (10 CFR 73.54), affected existing nuclear power reactor licensees and those corporations applying for new reactor licenses. The new regulation requires licensees to submit a new cyber security plan and an implementation timeline for NRC approval. The plan must show how the facility identified (or would identify) critical digital assets and describe its protective strategy, among other requirements.

Most recently, in January 2010, the NRC published a Regulatory Guide that provides comprehensive guidance to licensees and applicants for licenses on an acceptable way to meet the requirements of 10 CFR 73.54. The guidance includes recommended 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, as well as guidance from the Department of Homeland Security. This guide is publically available.

How the NRC Regulates Cyber Security

Power reactor licensees and those seeking permission to construct and operate new reactors must prove that their digital computer and communication systems and networks are protected against cyber attacks, including those systems and networks associated with:

- safety-related and important-to-safety functions,
- security functions,
- emergency preparedness functions, including offsite communications, and
- support systems and equipment important to safety and security.

To do this, they must submit a plan describing how the facility's cyber security program has been or will be established and maintained to meet the cyber security requirements added to 10 CFR. The plan is submitted to the NRC for review and approval and must account for any site-specific conditions that might affect implementation. The NRC cyber security staff then reviews it, and may need to ask for additional information as part of the review. If the NRC finds that the cyber security plan meets the requirements of 10 CFR 73.54, the staff issues a Safety Evaluation Report. Once approved, the plan becomes part of the site's operating license and is enforceable.

Ongoing Actions of the NRC Cyber Security Staff

Defending against hackers, criminals, and cyber terrorists is a complex endeavor that involves facing a changing and evolving threat. The NRC's cyber security 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 cyber security inspection program for future implementation. All sites will be required to satisfy those inspection requirements.

In addition, the NRC is collaborating with the Federal Energy Regulatory Commission, the North American Electric Reliability Corporation (NERC) and other organizations on cyber security. 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 cyber security oversight that extends from the plant itself to the electrical grid as a whole.

To be successful in combating the cyber threat, the NRC, and its government and private sector partners must continue to build on their relationships and make use of advances in technology. That partnering, when combined with the use of technology, helps ensure that cyber attacks at both prevented and deterred.

April 2010