

UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
OFFICE OF NUCLEAR MATERIAL SAFETY AND SAFEGUARDS  
OFFICE OF FEDERAL AND STATE MATERIALS AND  
ENVIRONMENTAL MANAGEMENT PROGRAMS  
OFFICE OF NUCLEAR REACTOR REGULATION  
OFFICE OF NEW REACTORS  
WASHINGTON, DC 20555-0001

October 13, 2009

NRC INFORMATION NOTICE 2009-24: SOURCES OF INFORMATION RELATED TO  
POTENTIAL CYBER SECURITY  
VULNERABILITIES

**ADDRESSEES**

All holders of operating licenses or construction permits for nuclear power reactors or non-power (research or test) reactors under the provisions of Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, "Domestic Licensing of Production and Utilization Facilities." All holders of operating licenses for Category I fuel cycle facilities, Category III fuel cycle facilities, conversion facilities, uranium recovery facilities, and enrichment facilities. All holders of, and applicants for, combined licenses under the provisions of 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants." All holders of licenses for the following types of facilities undergoing decommissioning: nuclear power plants, non-power reactors, fuel cycle facilities, and uranium recovery facilities.

**PURPOSE**

The U.S. Nuclear Regulatory Commission (NRC) is issuing this Information Notice (IN) to assist facility managers and other security and safety personnel responsible for protecting NRC-licensed facilities and radioactive materials when implementing cyber security requirements in accordance with 10 CFR Part 73, "Physical Protection of Plants and Materials"; NRC orders; and licensees' NRC-approved security plans. The NRC expects that all recipients will review the information for applicability to their facilities and consider implementing actions, as appropriate. However, suggestions contained in this IN are not NRC requirements and, therefore, require no specific action or written response.

**BACKGROUND**

Following the September 11, 2001, attacks, the NRC issued orders on February 25, 2002, that required power reactor licensees to take certain actions relative to digital computer and communication systems and networks to enhance cyber security at their sites. Subsequently, the NRC amended the design basis threat requirements in 10 CFR 73.1 to include cyber attacks. As licensees implement digital upgrades for many systems at their plants, the potential for adverse consequences from cyber threats will be increased. Cyber security, like physical security, focuses on the protection of equipment, systems, and networks against attacks by those individuals or organizations that would seek to cause harm, damage, or adversely affect the functions performed by such equipment, systems, and networks.

**ML083250226**

Nuclear facilities increasingly rely on computerized technology equipment relating to security and operating processes. The NRC encourages licensees to maintain effective processes and procedures at their facilities and to protect against a cyber attack to minimize vulnerabilities that may pose threats to the safety, security, and emergency response functions.

In May of 2008, the NRC issued Security Advisory (SA) 2008-05, "Potential Cyber Security Vulnerabilities." Even though the issues identified in SA 2008-05 did not challenge the safety, security, or emergency response functions at nuclear facilities, they provide insight into potential cyber vulnerabilities.

## DISCUSSION

This IN provides all recipients with Web sites that may be used to enhance their facility's cyber security program in an effort to be vigilant to cyber threats and vulnerabilities. Although there is no specific regulatory requirement to do so, licensees may refer to the Web sites in the list below for the best practices in cyber security that could limit vulnerabilities and opportunities for cyber attacks. On March 27, 2009, the final rule was published in the Federal Register [74 FR 13970] that added 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks," that specifies requirements for nuclear power plant licensees to establish, implement, and maintain a cyber security program. Power reactor licensees should note that any information contained within these Web sites that contradicts the requirements in 10 CFR 73.54, should not be utilized in implementing the sites' cyber security program.

1. The United States Computer Emergency Readiness Team (US-CERT) is a partnership between the U.S. Department of Homeland Security and the public and private sectors. Established in 2003 to protect the Nation's Internet infrastructure and control systems, US-CERT coordinates defenses against and responses to cyber attacks across the Nation. US-CERT's Web sites are:  
<http://www.us-cert.gov>  
[http://www.us-cert.gov/control\\_systems/](http://www.us-cert.gov/control_systems/)
2. InfraGard, the Federal Bureau of Investigation's outreach program, is an association of businesses, academic institutions, State and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. The InfraGard Web site is:  
<http://www.infragard.net>
3. In addition to US-CERT and InfraGard, there are many other useful Web sites that offer recommended secure computer use procedures and options for updates through e-mail subscriptions. Some of these additional Web sites include:  
<http://www.staysafeonline.org>  
<https://buildsecurityin.us-cert.gov/daisy/bsi/home.html>

Effective cyber security involves diligence in establishing and implementing appropriate security measures. Long-term cyber security effectiveness necessitates an understanding of both the changing technology and the nature of the cyber threat. This IN provides licensees with resources that may be consulted to enhance their facilities cyber security program in an effort to be vigilant to current and future cyber threats and vulnerabilities.

## CONTACT

This IN requires no specific action or written response. Please direct any questions about this matter to the technical contact listed below.

*/RA/*

Timothy J. McGinty, Director  
Division of Policy and Rulemaking  
Office of Nuclear Reactor Regulation

*/RA/*

Daniel H. Dorman, Director  
Division of Fuel Cycle Safety and Safeguards  
Office of Nuclear Material Safety and Safeguards

*/RA/*

Robert J. Lewis, Director  
Division of Materials Safety  
and State Agreements  
Office of Federal and State Materials and  
Environmental Management Programs

*/RA/*

Glenn Tracy, Director  
Division of Construction Inspection  
and Operational Programs  
Office of New Reactors

Technical Contact: F. Scot Sullivan, NSIR  
(301) 415-6107  
[Frederick.Sullivan@nrc.gov](mailto:Frederick.Sullivan@nrc.gov)

Note: NRC generic communications may be found on the NRC public Web site,  
<http://www.nrc.gov>, under Electronic Reading Room/Document Collections.

**CONTACT**

This IN requires no specific action or written response. Please direct any questions about this matter to the technical contact listed below.

***RA/***

Timothy J. McGinty, Director  
Division of Policy and Rulemaking  
Office of Nuclear Reactor Regulation

***/RA/***

Daniel H. Dorman, Director  
Division of Fuel Cycle Safety and Safeguards  
Office of Nuclear Material Safety and Safeguards

***/RA/***

Robert J. Lewis, Director  
Division of Materials Safety  
and State Agreements  
Office of Federal and State Materials and  
Environmental Management Programs

***/RA/***

Glenn Tracy, Director  
Division of Construction Inspection  
and Operational Programs  
Office of New Reactors

Technical Contact: F. Scot Sullivan, NSIR  
(301) 415-6107  
[Frederick.Sullivan@nrc.gov](mailto:Frederick.Sullivan@nrc.gov)

Note: NRC generic communications may be found on the NRC public Web site,  
<http://www.nrc.gov>, under Electronic Reading Room/Document Collections.

ADAMS Accession Number: ML083250226

OFFICE	RSOB:NSIR	TECH EDITOR	RSOB:NSIR	BC:RSOB:NSIR	BC:FCTSB:NSIR	BC:RSRLB:NSIR	DD:DSO:NSIR
NAME	FSullivan	KAzariah-Kribbs	RCostello	RAIbert	BCaldwell	CErlanger	BWestreich
DATE	10/27/08	11/21/08 email	06/02/09	10/28/08	10/30/08	10/24/08	01/07/09
OFFICE	D:DSP:NSIR	D:DSO:NSIR	OGC	D:NSIR	PGCB:DPR	PGCB:DPR	
NAME	RCorreia	PHolahan	JGoldberg	RZimmerman	DBeaulieu	CHawes	
DATE	10/24/08	01/08/09	07/06/09	8/14/09	10/2/09	10/05/09	
OFFICE	BC:PGCB:DPR	D:DMSSA	D:DCIP:NRO	D:FCSS:NMSS	D:DPR		
NAME	MMurphy	RLewis	GTracy	DDorman	TMcGinty		
DATE	10/13/09	09/04/09	09/29/09	12/04/08	10/13/09		

**OFFICIAL RECORD COPY**