POLICY ISSUE
INFORMATION

June 25, 2012 SECY-12-0088

FOR: The Commissioners

FROM: James T. Wiggins, Director
Office of Nuclear Security and Incident Response

SUBJECT: THE NUCLEAR REGULATORY COMMISSION CYBER SECURITY ROADMAP

PURPOSE:

The purpose of this paper is to update the Commission on the status of the U.S. Nuclear Regulatory Commission's (NRC's) implementation of cyber security requirements for power reactor licensees and combined operating license (COL) applicants. Additionally, this paper communicates the staff's approach, or roadmap, for evaluating the need for cyber security requirements for the following four categories of the NRC licensees and facilities: (1) fuel cycle facilities (FCFs); (2) non-power reactors; (3) independent spent fuel storage installations (ISFSIs); and (4) byproduct materials licensees.

SUMMARY:

The threat to NRC licensees from malicious cyber actors is persistent and evolving. In March 2009, the NRC issued Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54, "Protection of Digital Computer and Communication Systems and Networks." The cyber security rule applies to all power reactors and COL applicants. The experience gained in developing this rule and its associated framework provides an approach for developing similar cyber security requirements for other categories of licensees. The roadmap reflects a graded approach to developing cyber security requirements commensurate with the inherent nuclear safety and security risks associated with each type of licensee and facility. Additionally, this roadmap aligns with the current NRC strategic plan, which states that the NRC will manage the risk to information and systems to ensure the integrity of cyber security at regulated facilities.

CONTACT: Monika Coflin, NSIR/DSP
301-415-6659

BACKGROUND:

Following the terrorist attacks on September 11, 2001, the NRC issued a series of advisories and Orders requiring nuclear power plants to take certain actions, including enhancing the protection of certain computer systems (see Enclosure 1). Staff initiated the security rulemaking effort for power reactors in October 2006 (see 71 *Federal Register* 62663 dated October 26, 2006). The cyber security rule was initially created as a subsection of the 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage," rulemaking. However, upon further consideration, the staff decided to issue the cyber security rule as a separate section, 10 CFR 73.54. As explained in the statements of consideration for the final reactor security rule, this separate section was created to "enable the cyber security requirements to be made applicable to other types of facilities and applications through future rulemakings" (see 74 *Federal Register* 13933 dated March 27, 2009).

In March 2009, the NRC issued 10 CFR 73.54, requiring licensees and COL applicants to provide high assurance that digital computer and communication systems and networks associated with nuclear power plant safety, security, and emergency preparedness (SSEP) functions are protected from cyber attacks. The development of associated guidance for implementing the requirements in 10 CFR 73.54 resulted in the publication of Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities." RG 5.71 was developed for nuclear power plants and is based on cyber security standards and practices published by the National Institute of Standards and Technology, the U.S. Department of Homeland Security (DHS), the Institute of Electrical and Electronics Engineers, and the International Society of Automation. RG 5.71 also contains a generic template that licensees may use as guidance in developing their required cyber security plans (CSPs). RG 5.71 was developed with flexibility so that future revisions could be tailored for use by other categories of licensees and facilities.

Independent of the NRC's development of RG 5.71, the Nuclear Energy Institute (NEI) developed NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6. The NRC staff found NEI 08-09, Revision 6, acceptable for use by industry (Agencywide Documents Access and Management System Accession No. ML101190371) in meeting the requirements set forth in 10 CFR 73.54. This document provides another template that nuclear power plants can use when submitting CSPs to the NRC for review and approval. NEI 08-09, Revision 6, was reviewed to ensure that the document complied with the requirements set forth in 10 CFR 73.54. The staff intends to endorse NEI 08-09 via the next revision of RG 5.71. The update is scheduled to begin in fiscal year (FY) 2014.

Threat

Cyber threats to NRC licensees are dynamic and multi-dimensional due to the continuously evolving capabilities of potential adversaries and emerging technologies. Potential adversaries run the gamut from nation-state actors to individuals, i.e., "hacktivists." Recent threats against international nuclear facilities, such as Stuxnet and Duqu, are evidence of malware specifically targeting control systems that operate industrial facilities, such as nuclear power plants. In order to monitor the threat to U.S. nuclear facilities, the staff of the NRC's Intelligence Liaison and Threat Assessment Branch (ILTAB) has established formal liaison relationships with the National Counterterrorism Center, the DHS U.S. Computer Emergency Response Team

(US-CERT), and the Federal Bureau of Investigation, among others. It also has frequent informal liaisons with all major intelligence community and law enforcement agencies. ILTAB regularly monitors the threats associated with cyber security, including potential threats against licensed facilities, and shares cyber threat information through numerous mechanisms, including bi-weekly threat briefings, periodic finished intelligence products, and an annual assessment of kinetic (i.e., physical attack using conventional or unconventional explosives) and non-kinetic threats (i.e., cyber-enabled attack that may or may not result in physical damage depending on intent of sponsor and/or unintended consequences).

Involvement with Federal/International Partners and Stakeholders

The NRC coordinates with Federal partners and international stakeholders on cyber security issues through a variety of technical meetings, working groups, workshops, and conferences. NRC staff regularly reviews and provides comments on international cyber security documents, such as the International Atomic Energy Agency's Nuclear Security Series documents, and continues to make a concerted effort to coordinate with the international nuclear community regarding cyber security. Staff regularly participates in interagency working groups, such as the Industrial Control Systems Joint Working Group and the Cross-Sector Cyber Security Working Group, both established by DHS. NRC staff also regularly participates in industry working groups, such as the NEI-led Cyber Security Task Force.

The NRC formed a cyber assessment team (CAT) to provide a consistent process for evaluation and resolution of issues with potential cyber security-related implications for all NRC licensees. The CAT is staffed by experts in cyber security, digital instrumentation and control, and other disciplines from across the agency and the Regions. These experts support the NRC and its mission by promptly addressing, assessing, and evaluating cyber security-related issues that could impact the NRC licensees' computers, communication systems, and networks associated with SSEP functions. The CAT provides recommendations and/or a course of action to the appropriate program office and NRC management. In accordance with the National Cyber Security Incident Response Plan, the NRC CAT coordinates and communicates with the DHS Industrial Control Systems Cyber Emergency Response Team and the US-CERT on a regular basis.

The NRC is actively engaged in cyber security research exploring cyber vulnerabilities. This research will ultimately provide improved regulatory guidance and tools for evaluating digital systems and networks for cyber vulnerabilities, including potential vulnerabilities arising from safety and non-safety system interconnections.

DISCUSSION:

The NRC's strategic plan for FYs 2008 through 2013 states that the NRC will manage the risk to information and systems to ensure the integrity of cyber security at regulated facilities. The NRC is currently achieving this goal for power reactor licensees and COL applicants through the implementation of 10 CFR 73.54.

This section provides a status of cyber security activities at nuclear power plants and outlines the actions that the staff is taking to determine the appropriate regulatory actions needed to ensure the goal of managing risk to information and digital systems at FCFs, non-power

reactors, ISFSIs, and byproduct materials licensees. The proposed activities are graphically depicted in Enclosure 2. The NRC is pursuing a parallel vice sequential approach to implementing this cyber security roadmap and, throughout the process, is sharing lessons learned from licensees and facilities.

Reactor Licensees and COL Applicants

NRC's cyber security regulation requires operating reactor licensees and COL applicants to provide high assurance of adequate protection against cyber security attacks for nuclear power plant SSEP functions, up to and including the design basis threat (DBT). All operating nuclear power plant licensees submitted a CSP and proposed an implementation schedule to the Commission for review and approval by November 23, 2009. The NRC reviewed and approved all licensee submitted CSPs and implementation schedules. Presently, licensees are working to implement their cyber security programs, and the NRC is developing inspection guidance documents and the oversight program to verify compliance with the approved CSPs. Oversight activities performed by the NRC, including cyber security inspections, will be conducted by trained and qualified headquarters and regional NRC inspectors.

In accordance with 10 CFR 73.54, COL applicants are required to submit a CSP as part of the process for acquiring an operating license. Applicants submit their respective CSPs on a timeline that is consistent with their overall licensing schedule. The NRC has reviewed and approved the CSPs for Vogtle Units 3 and 4, and Summer Units 2 and 3. The NRC also added a license condition that requires Vogtle Units 3 and 4, and Summer Units 2 and 3 to submit a cyber security implementation schedule that supports planning for, and conduct of, NRC inspection of the cyber security program implementation no later than 12 months after the license is granted. The NRC intends to impose this license condition for future COLs as well.

Staff is currently updating 10 CFR 73.71 "Reporting of Safeguards Events," and Appendix G to Part 73 "Reportable Safeguards Events" to address cyber security. The proposed appendix to the rule adds security event reporting and recording requirements related to certain cyber security issues at nuclear power reactor facilities (see 76 *Federal Register* 6200 dated February 3, 2011). The public comment period closed on August 2, 2011.

FCFs

The fuel cycle is comprised of a broad spectrum of facility types and processes. Therefore, there are a wide variety of potential vulnerabilities and consequences resulting from a cyber attack. The special nuclear material at FCFs presents risks such as proliferation, diversion, theft, sabotage, and criticality safety. Currently, all FCFs are under additional security measures (ASM) orders to address certain security risks, including cyber security. The two category I facilities under NRC regulatory jurisdiction are required by 10 CFR 73.1, "Purpose and Scope," to address cyber security as part of their DBTs.

The staff began examining potential cyber vulnerabilities at FCFs in FY 2011, and issued a questionnaire to FCF licensees requesting information about the FCFs' safety, material control and accountability, security (physical and information), and emergency preparedness digital assets. Subsequently, the NRC conducted four site visits at a cross section of FCFs to evaluate

the information submitted in the questionnaires and observe how the digital assets at these facilities are used and protected.

The staff recognizes that not all FCFs are the same and that not all digital assets will require the same level of protection. As a result, in January 2012, staff determined that a rulemaking using a graded, risk-informed approach to address cyber security for digital assets at FCFs should be considered. The staff plans to submit a SECY paper in FY 2013 seeking Commission approval for the staff to initiate the rulemaking process. In the short-term, the NRC is working with NEI and FCF licensees on a voluntary industry initiative that would strengthen licensee cyber security programs. However, if industry decides not to participate in this voluntary initiative or if the resulting changes do not generate the desired outcome of strengthening existing FCF cyber security programs, Orders will be considered.

Non-Power Reactors

Non-power reactor designs vary significantly as a function of maximum licensed power levels; the operating duration and frequency of the reactor; and the quantity, enrichment, and form of nuclear materials maintained at the facility. These differences lead to a significant variation in fission product inventory, which is a primary factor in determining the potential hazards and accident consequences presented by non-power reactors to public health and safety. Also unique to non-power reactors is the direction provided in the Atomic Energy Act of 1954 (AEA), as amended, Section 104.c, which states:

> The Commission is directed to impose only such minimum amount of regulation of the licensee as the Commission finds will permit the Commission to fulfill its obligations under this Act to promote the common defense and security and to protect the health and safety of the public and will permit the conduct of widespread and diverse research and development.

In November 2011, the NRC issued a guidance document to assist non-power reactor operators in performing a self-assessment of the vulnerability of their facility to cyber attack. This document was discussed with the National Organization of Test Research and Training Reactors' (TRTR) executive committee and several other stakeholders who expressed an interest in providing a coordinating role in the implementation of these self-assessments.

The staff's current view is that the diverse nature of non-power reactor designs and the direction in the AEA for imposition of the minimum regulation makes it necessary to apply a graded approach to cyber security. In the third and fourth quarters of FY 2012, non-power reactor licensees are scheduled to conduct self-assessments and the TRTR will report the results to the NRC. In the fourth quarter of FY 2012, the staff plans to evaluate the self-assessment results and identify three to five sites for assessment visits. The staff anticipates completing the site visits in the second quarter of FY 2013. In the second and third quarters of FY 2013, the staff plans to review site assessment results, discuss these results with stakeholders, identify and analyze options, and determine the next steps. If the staff concludes rulemaking is necessary, the staff will first provide the basis for that conclusion to, and seek approval from, the Commission before further proceeding with rulemaking activities. The timeline for rulemaking activities will be determined in accordance with the agency's common rulemaking prioritization process.

ISFSIs

By regulation, dry cask storage in ISFSIs allows spent fuel that has already been cooled in the spent fuel pool for 1 year to be surrounded by inert gas inside a storage cask. Licensees that are subject to 10 CFR 72.212, "Conditions of General License Issued Under § 72.210," (i.e., licenses limited to storage of spent fuel in casks) must also comply with specific portions of 10 CFR 73.55 requirements for physical security and the ASM Orders, but are not subject to the provisions of 10 CFR 73.54, which specifically applies to operating reactors and COL applicants.

The NRC staff plans to form a working group in the fourth quarter of FY 2012 to determine if the potential threat to ISFSIs' systems warrants protection from cyber attack. The staff plans to conduct an ISFSI cyber security assessment focusing on vulnerability and consequence analysis for each of the three types of ISFSIs: within an operating reactor protected area (PA), co-located with the operating reactor outside the reactor PA, and not co-located with an operating reactor (i.e., standalone/decommissioned). The staff also plans to conduct site visits beginning in the second quarter of FY 2013. In the third and fourth quarters of FY 2013, the staff intends to review site assessment results, discuss these results with stakeholders, identify and analyze options, and make a determination on the next steps required to ensure that ISFSI digital security systems are adequately protected from cyber attacks.

Byproduct Materials

Developing the cyber security requirements for radioactive materials licensees is complex, due to the thousands of licensees involved, and the variety of different operating environments with unique characteristics and different risks. Materials licensees operate in environments that vary from large manufacturing facilities, universities, and medical facilities to small industrial radiography businesses. A vulnerability and consequence analysis for the different groups of materials licensees is necessary to determine appropriate levels of protection. Additionally, the majority of materials licensees are regulated by the Agreement States.

Another consideration is the role of the Food and Drug Administration (FDA) in regulating the manufacturers of medical devices that use radioactive materials. The FDA has issued two guidance documents for industry that provide voluntary best practices for software assurance and cyber security for digital devices. On December 4, 2002, an existing memorandum of understanding (MOU) between the FDA and the NRC was renewed. The MOU clarifies the respective roles of each agency in regulating the safe use of radiopharmaceuticals and sealed sources, or devices containing radioactive material, and is designed to foster cooperation between the two agencies, as well as to provide for more effective exchanges of information. As a result, the NRC and the FDA have established liaison officers and identified key management and technical personnel for coordinating responses to emergencies or specific events of mutual interest. The NRC and the FDA have conducted joint inspections of medical events involving device failures and human or computer-generated errors. The FDA has expressed an interest in the NRC's cyber security efforts with respect to materials licensees. The NRC plans to share information on these efforts with the FDA within the context of the existing MOU.

In the fourth quarter of FY 2012, the NRC staff plans to form a working group with Agreement State participation (Materials Cyber Security Working Group) in accordance with Management Directive 5.3, “Agreement State Participation in Working Groups,” Section III, “Internal NRC Working Groups,” as part of the process of developing regulatory requirements.

The Materials Cyber Working Group will focus initially on developing a set of self-assessment tools to aid licensees in gathering information from a small sample group representing a variety of materials licensees. Development of assessment materials is expected to be completed in the fourth quarter of FY 2012. In the first quarter of FY 2013, the representative sample group of licensees will conduct the self-assessments and report the results to the working group. During the second and third quarters of FY 2013, the working group will assess the results and participate in a limited number of site visits. The working group will then review the results of the assessments and site visits and prepare a paper outlining actions for consideration by the first quarter of FY 2014. If the working group recommends rulemaking, the timeline for rulemaking activities will be in accordance with the agency’s common prioritization process.

RESOURCES:

The staff anticipates that it has sufficient resources to conduct all the cyber security related roadmap activities outlined in this paper for the remainder of FY 2012. For the agency, the FY 2013 President’s Budget includes $350K and 1.2 full-time equivalent for these cyber security roadmap activities. For FY 2014 and beyond, the staff will use the Planning, Budget, and Performance Management process to request the resources necessary to implement the cyber security roadmap activities described in this paper.

COORDINATION:

The Office of the General Counsel reviewed this information paper and has no legal objection. The Office of the Chief Financial Officer has reviewed this paper for resource implications and has no objections.

CONCLUSION:

The NRC has a number of risk-informed, performance-based security programs in place to effectively protect our Nation’s commercial nuclear facilities. Recent high-profile attacks such as Stuxnet, combined with a general interest by U.S. lawmakers on cyber security requirements for all sectors of the Nation’s critical infrastructure, underscore the importance of evaluating cyber security requirements for all classes of NRC licensees. The NRC has existing requirements, effective processes, the expertise to regulate cyber security, and an established foundation as a result of the development and implementation of 10 CFR 73.54. This experience with power reactors has positioned the agency to develop requirements promptly

and effectively for other types of licensees. The implementation of this roadmap will ensure that appropriate levels of cyber security actions are implemented in a timely and efficient manner at all NRC licensed facilities and identify if any program improvements are needed.

/RA/

James T. Wiggins, Director
Office of Nuclear Security and
Incident Response

Enclosures:
1. Timeline of NRC Actions to Address Cyber Security
2. Milestone Matrices

TIMELINE OF NUCLEAR REGULATORY COMMISSION (NRC) ACTIONS TO ADDRESS CYBER SECURITY

In response to the terrorist attacks of September 11, 2001, and subsequent information provided by intelligence and law enforcement agencies, the NRC took the following actions to protect against cyber-based threats.

- 2001: Issued a security advisory to power reactors to enhance cyber security.
- 2003: Issued a security order (Title 10 of the *Code of Federal Regulations* (10 CFR) 73.1) defining the design basis threat (DBT).
- 2004: Published NUREG/CR-6847, "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants."
- 2005: Endorsed Nuclear Energy Institute (NEI) 04-04, "Cyber Security Program for Power Reactors."
- 2006: Developed security criteria for use of computers in safety systems (Regulatory Guide (RG) 1.152, Revision 2).
- 2007: Published guidance on software reviews for digital instrumentation and control systems (Branch Technical Position 7-14, Revision 5).
- 2007: Added a cyber threat component to the DBT.
- 2009: Published 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks," to provide high assurance that nuclear power plant safety, security, and emergency preparedness functions were protected from cyber attacks.
- 2010: Published RG 5.71, "Cyber Security Programs for Nuclear Facilities," for licensee use to meet the requirements of 10 CFR 73.54.
- 2010: Found NEI 08-09, Revision 6, "Cyber Security Plan for Nuclear Power Reactors," acceptable for use to meet the requirements of 10 CFR 73.54.

Enclosure 1

MILESTONE MATRICES

Class of Licensee	Likely Roadmap Major Milestones for NRC-Licensed Facilities Other Than Power Reactors												
	FY2011 Q1	FY2011 Q2	FY2011 Q3	FY2011 Q4	FY2012 Q1	FY2012 Q2	FY2012 Q3	FY2012 Q4	FY2013 Q1	FY2013 Q2	FY2013 Q3	FY2013 Q4	FY2014 Q1
Fuel Cycle Facilities (FCFs):	Initial NRC staff evaluation	Questionnaire issued and (4) site visits conducted				NRC staff analysis completed/ Office Directors briefed	Licensee-initiated measures to address potential cyber security threats / Orders considered					If approved, initiate Rulemaking →	
Non-Power Reactors:	NRC Issued Guidance Document						Licensees conduct self-assessments and report results to NRC			NRC staff complete 3-5 site assessment visits			
								NRC staff evaluate self-assessment results		NRC staff review site assessment results, complete analysis, determine next steps →			
Independent Spent Fuel Storage Installations (ISFSIs):								Establish Cyber Working (WG) Group		Begin site visits	NRC staff review site assessment results, complete analysis, determine next steps →		
Byproduct Materials Licensees:								Establish Cyber WG and develop assessment materials	Licensees conduct self-assessments and report results to WG	WG assess results and participate in site visits	NRC staff review site assessment results, complete analysis, determine next steps →		

Enclosure 2

Likely Roadmap Major Milestones for NRC-Licensed Facilities (Power Reactors)

FY2012 Q3	FY2012 Q4	FY2013 Q1	FY2013 Q2	FY2013 Q3	FY2013 Q4	FY2014 Q1	FY2014 Q2	FY2014 Q3	FY2014 Q4
		Complete Develop-ment of Inspection Program	NRC begin inspection of interim implementation of operating reactors' cyber security program						NRC begin inspection of full implementa-tion of operating reactors' cyber security program
						NRC Begin Update of Regulatory Frame-work*			

*Update of Regulatory Framework includes updating RG 5.71 to incorporate lessons learned and endorsing NEI 08-09, Rev. 6 and NEI 10-04 via RG 5.71