POLICY ISSUE
(Information)

February 28, 2017 SECY-17-0034

FOR: The Commissioners

FROM: Victor M. McCree
Executive Director for Operations

SUBJECT: UPDATE TO THE U.S. NUCLEAR REGULATORY COMMISSION CYBER SECURITY ROADMAP

PURPOSE:

The purpose of this paper is to provide the Commission with an update on the implementation of cyber security requirements for both operating reactors and combined license (COL) holders. Additionally, this paper provides an update on the staff's evaluation of the appropriate cyber security requirements for the following four categories of the U.S. Nuclear Regulatory Commission (NRC) licensees and regulated facilities: (1) fuel cycle facilities (FCFs); (2) non-power reactors (NPRs); (3) independent spent fuel storage installations (ISFSIs); and (4) byproduct materials licensees. Finally, this paper also discusses the application of the NRC's cyber security requirements to decommissioning reactors. This paper does not address any new commitments and does not present a change in cyber security strategy for any category of licensee or regulated facility.

SUMMARY:

Recent high-profile cyber attacks, such as the December 2015 attack on the Ukraine's power grid, underscore the importance of continuing to evaluate the need for a cyber security regulatory framework for all classes of NRC licensees. The NRC has gained in-depth experience with cyber security as a result of the development, implementation, and inspections performed under Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54. The NRC's oversight of cyber security implementation at operating reactors has positioned the agency to develop, as needed, cyber security regulations, or other measures, for various types of NRC licensees. The continued implementation of the cyber security roadmap will help (1) ensure that appropriate levels of cyber security actions are implemented in a timely and efficient manner at all NRC and Agreement State licensed facilities, and (2) identify any needed improvements.

CONTACT: James Beardsley, NSIR/DSP/CSB
301-287-0908

BACKGROUND:

Following the terrorist attacks on September 11, 2001, the NRC issued a series of security advisories and orders requiring nuclear power plants to take certain actions, including enhancing the protection of certain computer systems.

In March 2009 the NRC issued 10 CFR 73.54, requiring operating reactors and COL applicants to ensure that digital computer and communication systems associated with a nuclear power plant's safety, security, and emergency preparedness (SSEP) functions are protected from cyber attacks. The NRC issued guidance on implementing the requirements of 10 CFR 73.54, in Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," in January 2010 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML090340159). The Nuclear Energy Institute (NEI) also published implementing guidance in NEI 08-09, "Cyber Security Plan for Nuclear Power Plants." These documents provided information to aid licensees in developing Cyber Security Plans (CSPs).

On June 25, 2012, the NRC issued SECY 12-0088, "The Nuclear Regulatory Commission Cyber Security Roadmap" (ADAMS Accession No. ML12135A050). This roadmap laid out a graded approach for implementation of the NRC's cyber security requirements for power reactor licensees and communicated the staff's approach to evaluating the need for cyber security requirements for other NRC-regulated facilities.

Threat

Cyber threats to NRC licensees are dynamic due to emerging technologies and the continuously evolving capabilities of potential adversaries. Adversaries are becoming increasingly aware of the offensive opportunities presented by vulnerabilities in key infrastructure sectors. Nation states have demonstrated a willingness to target critical infrastructure systems to achieve their strategic and tactical goals. Such threats are accentuated by the internationalization of U.S. supply chains and service infrastructure.

Involvement with Federal/International Partners and Stakeholders

The NRC regularly monitors the threats associated with cyber security, including potential threats against NRC licensed facilities. As such, the NRC has established liaison relationships with the intelligence and law enforcement communities to include the National Counterterrorism Center, the Department of Homeland Security's U.S. Computer Emergency Response Team, and the Federal Bureau of Investigation.

The NRC participates with other government regulators on the Cybersecurity Forum for Independent and Executive Branch Regulators (the Forum). The NRC Chairman served as the first Chair of the Forum and, in September 2016, turned the Chair over to the Federal Communications Commission. The purpose of the Forum is to increase the overall effectiveness and consistency of regulatory authorities' cyber security efforts pertaining to U.S. critical infrastructure. The Forum enhances communication among regulatory agencies, regulated entities, and other organizations by sharing best practices and gathering expertise in this rapidly changing field, including areas of cyber security risk assessment, information sharing, and both voluntary and regulatory approaches to cyber security.

The NRC staff coordinates with international stakeholders on cyber security issues through a variety of technical meetings, working groups, workshops, and conferences. The staff regularly participates in consultancy meetings with the International Atomic Energy Agency on development of its nuclear security series of documents affecting cyber security.

DISCUSSION:

NUREG 1614 Volume 6, "NRC: Strategic Plan: Fiscal Years 2014-2018" (ADAMS Accession No. ML14246A439) states that the NRC will ensure that cyber security guidance for NPRs remains informed by operating experience and monitoring of the cyber security threat environment. It further states that the NRC will evaluate the need for cyber security requirements for FCFs, ISFSIs, NPRs, nuclear facilities being decommissioned, and other materials licensees. The following sections provide an update on the status of cyber security activities at nuclear power plants, including actions the staff is taking to ensure that cyber security guidance remains informed by operating experience and monitoring of the threat environment. Also included is an update on rulemaking activities for FCFs, as well as a summary of the ongoing evaluation of the need for an appropriate cyber security regulatory framework for other types of NRC-regulated facilities.

Operating Reactor Licensees and Combined License Holders

The NRC's cyber security regulation (10 CFR 73.54) requires operating reactor licensees and COL applicants to ensure 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. Subsequently, the NRC approved revisions to the schedules that provided for a phased approach to the implementation of CSP requirements. This phased approach established 8 Milestones. Phase 1, implementing Milestones 1 through 7, was completed by December 31, 2012. Phase 2, implementation of Milestone 8, will result in full compliance with the licensee's CSP. The implementation date for Milestone 8 varies by licensee (a brief description of each milestone is included in Appendix A). The phased implementation and milestones ensured that an initial level of protection against cyber security threats was achieved prior to full implementation of the cyber security program required by 10 CFR 73.54.

Milestones 1-7 were completed at all operating reactor sites in 2012. Between 2013 and 2015 the NRC inspected each licensee to ensure that its initial level of protection was adequate. An evaluation of the lessons learned from these inspections is on-going; however, issues were identified in three key areas:

- Some licensees did not properly identify all of the equipment that should be considered a critical digital asset (CDA). Some incorrectly determined that either the equipment was not within the scope of the cyber rule or they failed to identify the digital capabilities of the device.
- Some licensees did not properly implement security controls for some portable media and mobile devices (PMMD). Some of the identified issues included lack of physical control over the devices, not properly scanning and verifying the integrity of the data on the PMMD, preventing movement of PMMD between security levels, and a lack of training and procedures for how these devices were to be controlled.
- Some licensees did not properly identify and implement security controls for all CDAs

that affect critical plant equipment. Either the methodology used to determine if equipment was critical was not used or was used incorrectly. In addition, once a CDA was identified, the controls used to protect it were not always properly applied.

Beginning in 2016 and through 2017 the NRC staff is conducting corrective action inspections to ensure the issues identified during the Milestone 1-7 inspections have been addressed. In addition, the NRC staff has been working to address guidance issues through the use of the Security Frequently Asked Questions (SFAQ) process.

Presently, the operating reactor licensees are working to complete Milestone 8 (i.e., full implementation of their cyber security program). Due to the complexity of full compliance with 10 CFR 73.54, licensees have revised their specific implementation schedules such that full compliance will not be achieved for most licensees until December 2017. The NRC staff is developing an oversight program and inspection guidance documents to verify proper implementation of the approved CSPs. The staff has also developed advanced cyber security inspector training to ensure that qualified headquarters and regional NRC inspectors have up-to-date guidance.

The NRC staff has interacted extensively with the industry in preparation for full cyber security implementation. The first engagement was completed in April 2016 and discussed implementation of the NEI 13-10, Rev. 4, “Cyber Security Control Assessments.” NEI 13-10, Rev. 4 is approved by the NRC for use by licensees to apply the proper cyber controls based on a consequence-based approach. Additional interactions focused on monitoring and assessment controls; detection, response, and elimination requirements; supply chain requirements; and drills and training requirements. Lessons learned from the engagements will be captured in industry guidance documents, SFAQs, or other means as appropriate. Regional inspectors participated in all of these engagement activities. The staff anticipates that regional inspector participation in these interactions will result in greater consistency in the inspections of cyber security program implementation.

In accordance with 10 CFR 73.54, COL applicants are required to submit a CSP as part of their license application and COL holders are required to have their cyber security program fully implemented prior to fuel receipt. Westinghouse has been contracted by both Vogtle Units 3 and 4 (Vogtle) and Virgil C. Summer Units 2 and 3 (Summer) for initial development of their CSPs during the construction phases. The licensees retain oversight of the programs and are ultimately responsible for their implementation. Vogtle, Summer, and the NRC staff are working collaboratively to identify opportunities for early engagement to ensure that their cyber security programs are being properly developed and implemented. No other sites with a COL have started construction yet.

In November 2015 the NRC promulgated 10 CFR 73.77, “Cyber Security Event Notifications.” This rule requires licensees to report and record certain cyber security issues at operating reactors. Operating reactor licensees were required to be in full compliance with 10 CFR 73.77 by May 2, 2016 (80 FR 67264). The NRC published the associated guidance document, Regulatory Guide 5.83, “Cyber Security Event Notifications,” with the new rule. NEI developed and issued guidance for implementation of 10 CFR 73.77 in NEI 15-09, “Cyber Security Event Notifications.” The NRC has found NEI 15-09 acceptable for use to: (1) streamline the process for making notification determinations; (2) allow for consistent implementation of the cyber security event notifications final rule; and (3) provide additional examples of reportable events.

Next Steps for Operating Reactors and COL Holders: Operating reactor licensees are

scheduled to complete full implementation (i.e., Milestone 8) by December 2017. The NRC staff will conduct full implementation inspections beginning in Summer 2017 and continuing for approximately 3 years. The NRC staff will continue to engage with COL holders as they implement their CSPs prior to fuel receipt.

Fuel Cycle Facilities

The FCF licensees comprise a broad spectrum of facility types and processes. The special nuclear material and hazardous chemicals at FCFs present safety and security concerns that could lead to potential consequences of concern such as diversion, theft, sabotage, and radiological or chemical release as a result of a cyber attack. Currently, FCF licensees are under interim compensatory measures orders to address certain security threats, including a cyber attack. The two Category I FCF licensees under NRC regulatory jurisdiction are also required to protect against the DBT as described in 10 CFR 73.1, "Purpose and Scope," which includes a cyber attack as an element of the DBT.

On March 24, 2015, the Commission issued staff requirements memorandum SRM-SECY-14-0147, "Cyber Security for Fuel Cycle Facilities" (ADAMS Accession No. ML15083A175), which directed the staff to initiate an expedited cyber security rulemaking for FCF licensees. The staff engaged with external stakeholders and developed the regulatory basis document (ADAMS Accession No. ML15355A461).

Next Steps for FCF Licensees: The staff continues to engage with external stakeholders on the development of the proposed rule for cyber security for FCFs, which the staff expects to provide to the Commission in Spring 2017.

Non-Power Reactors

NPR designs vary significantly both in terms of maximum licensed power levels and in the quantity, enrichment, and form of nuclear materials maintained at the facility. In 2012 the NRC formed a working group that included representation from the National Organization of Test Research and Training Reactors. The working group had the following goals: (1) gather information concerning the cyber security protection currently in place at NPR facilities through licensee self-assessments; (2) conduct surveys to validate information provided in the licensee self-assessments; and (3) analyze the self-assessments and survey information within the framework of the risk posed to the public health and safety.

Following receipt of the licensee self-assessments in 2013 and 2014, the working group conducted site visits at four representative NPR facilities to determine what measures are in place to protect CDAs from cyber attacks, and whether the NRC needs to take any action to require licensees to strengthen their programs. Based on the site visit observations and assessments, the working group concluded that NPR licensees have implemented an adequate level of cyber security at their facilities. The working group developed and published a guidance document, "Cyber Security: Effective Practices for the establishment and maintenance of adequate cyber security at Non-Power (Research and Test) Reactor facilities" (ADAMS Accession No. ML15252A236), which provides NPR licensees with information about how to utilize instrument and control technologies and modern computer/networking technologies in a manner that provides adequate cyber security protection and mitigates the risks from cyber-based threats.

Next steps for NPRs: The staff is currently evaluating an all-digital hypothetical NPR model and conducting a cyber security assessment to determine if any identified vulnerabilities could lead to an unacceptable radiological consequence. This evaluation should be completed in 2017. Based on the results of the assessment, the staff will determine the need for any further regulatory action and will engage with the Commission as appropriate. The staff's evaluation of the application of cyber security regulations to NPRs does not take into account facilities that have indicated plans to produce Molybdenum-99 (Moly-99). The staff is evaluating the need for guidance on cyber security for the Moly-99 facilities.

Independent Spent Fuel Storage Installations

Spent fuel that has already been cooled in the spent fuel pool is typically placed in a storage cask surrounded by inert gas and stored at an ISFSI. Licensees that are subject to 10 CFR 72.212, "Conditions of General License Issued Under 10 CFR 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 additional security measures orders, but are not subject to the provisions of 10 CFR 73.54, which specifically applies only to operating reactors and COL holders.

In 2012 the staff formed a working group and conducted a study of cyber security protections at three ISFSIs to determine if the potential cyber threats to ISFSI systems warrant additional cyber protections. The staff determined, at that time, that the licensee's cyber security efforts adequately protect the ISFSIs from a cyber attack.

Next steps for ISFSIs: The NRC plans to re-evaluate the physical security protections at ISFSIs in 2020 to determine if rulemaking is warranted. This is consistent with staff recommendations in COMSECY-15-0024, "Proposed Rulemaking on Security Requirements for Facilities Storing Spent Nuclear Fuel and High-Level Radioactive Waste," dated September 11, 2015 (ADAMS Accession No. ML15229A231), and the associated Commission direction. Although not specifically stated in COMSECY-15-0024, the NRC staff intends to include cyber security as part of this re-evaluation.

Decommissioning Power Plants

Once a licensee has entered decommissioning, spent fuel is removed permanently from the reactor, temporarily stored in the spent fuel pool, and eventually transferred to an ISFSI. The licensee then must file the certifications required by 10 CFR 50.82, "Termination of License." Once the NRC dockets these certifications, the licensee is no longer authorized to operate a nuclear power plant.

The requirements in 10 CFR 73.54 apply to "each licensee currently licensed to operate a nuclear power plant under Part 50." Accordingly, consistent with the regulatory language, the requirements in 10 CFR 73.54 no longer apply to the licensee. However, any such licensee remains subject to its CSP license condition until that condition has been removed from their license pursuant to a 10 CFR 50.90 amendment request.

Next Steps for Decommissioning Power Plants: The staff is evaluating license amendment requests to remove the license conditions on a case-by-case basis.

Byproduct Materials

Developing 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 risks.

On January 6, 2016, the staff submitted a memorandum to the Commission titled “Staff Activities Related to the Evaluation of Materials Cyber Security Vulnerabilities” (ADAMS Accession No. ML15201A509). This memorandum informed the Commission of the on-going evaluation of the need for cyber security requirements for Categories 1 and 2 radioactive materials licensees.

In the memorandum, the staff described a two-pronged approach focused on information gathering and consequence analysis. For information gathering, the staff distributed a Cyber Security Survey Questionnaire (ADAMS Accession No. ML15246A306) on April 29, 2016, to all NRC and Agreement State licensees that possess Categories 1 and 2 quantities of radioactive materials.

The purpose of the questionnaire was to identify what key digital systems exist at each licensee type, how they are connected to internal/external networks and the internet, and identify technical and procedural security measures in place for protection of these systems. Questionnaire results were received in May 2016. The NRC received over 180 responses, which equates to about 10 percent of all byproduct licensees. In parallel with assessing the results from the information gathering effort, the working group is evaluating the potential for onsite and offsite consequences that may occur if the availability, integrity, or confidentiality of data or systems associated with Categories 1 and 2 quantities of radioactive materials were compromised by a cyber attack. The working group is developing a matrix, by licensee type, with potential impacts to digital assets that may need protection from cyber threats.

Next Steps for Byproduct Materials: The working group plans to complete its evaluation of the questionnaire responses, its consequence analysis, and any follow-up communication with stakeholders in early 2017. As a result, the working group intends to develop recommendations for a path forward by spring/summer 2017.

CONCLUSION:

Recent high-profile attacks such as the attack on the Ukraine’s power grid underscore the continued importance of determining the need for an appropriate cyber security regulatory framework for all classes of NRC licensees. The NRC has gained valuable experience in addressing cyber security threats at operating reactors as a result of the development, implementation, and inspections performed under 10 CFR 73.54. This experience with operating reactors has positioned the agency to determine the need for a cyber security regulatory framework for other types of licensees, as needed. The continued implementation of this roadmap will help (1) ensure that appropriate levels of cyber security actions are implemented in a timely and efficient manner at all NRC and Agreement State licensed facilities, and (2) identify any needed improvements.

RESOURCES:

Resources to support the roadmap activities are included in the current budget for fiscal year (FY) 2017 and the FY 2018 budget estimate. Resources in FY 2019 and beyond will be addressed using the agency's Planning, Budget, and Performance Management process.

COORDINATION:

The Office of the General Counsel reviewed this information paper and has no legal objection.

/RA/

Victor M. McCree
Executive Director
for Operations

Enclosure: Appendix A

RESOURCES:

Resources to support the roadmap activities are included in the current budget for fiscal year (FY) 2017 and the FY 2018 budget estimate. Resources in FY 2019 and beyond will be addressed using the agency's Planning, Budget, and Performance Management process.

COORDINATION:

The Office of the General Counsel reviewed this information paper and has no legal objection.

/RA/

Victor M. McCree
Executive Director
for Operations

Enclosure: Appendix A

ADAMS Accession No.: ML16354A258 Package No.: ML16354A282

OFFICE	NSIR/DSP/CSD	NSIR/DSP/CSD	NSIR/DSP	QTE	NRR
NAME	M. Brown	J. Beardsley	J. Andersen	J. Dougherty	W. Dean
DATE	12/18/16	12/18/16	12/20/16	01/11/17	01/27/17
OFFICE	NMSS	NRO	OGC	NSIR	EDO
NAME	M. Dapas	V. Ordaz	L. London	B. Holian	V. McCree
DATE	01/18/17	01/12/17	01/23/17	02/01/17	02/28/17

OFFICIAL RECORD COPY