POLICY ISSUE
(Notation Vote)

February 02, 2021 SECY-21-0011

FOR: The Commissioners

FROM: Margaret M. Doane
Executive Director for Operations

SUBJECT: DENIAL OF PETITION FOR RULEMAKING ON PROTECTION OF DIGITAL COMPUTER AND COMMUNICATION SYSTEMS AND NETWORKS (PRM-73-18; NRC-2014-0165)

PURPOSE:

To request Commission approval to publish the enclosed *Federal Register* notice (FRN) (Enclosure 1) denying a petition for rulemaking (PRM) submitted by the Nuclear Energy Institute (NEI) requesting amendment of the cyber security regulations in Title 10 of the *Code of Federal Regulations* (10 CFR) Section 73.54, "Protection of digital computer and communication systems and networks." This paper does not address any new commitments or resource implications.

BACKGROUND:

Anthony Pietrangelo, on behalf of NEI (the petitioner), filed a PRM with the U.S. Nuclear Regulatory Commission (NRC) on June 12, 2014 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML14184B120). The petitioner requested that the NRC amend its power reactor cyber security regulations to make them consistent with the original intent of the rule and clarify that the scope of those regulations only require the protection of those digital assets that, if compromised, can directly cause core damage and spent fuel sabotage, or whose failure would cause a reactor scram.

CONTACTS: Juan A. Lopez, NMSS/REFS
301-415-2338

Kim S. Holloway, NSIR/DPCP
301-415-0286

The NRC assigned docket number PRM-73-18 to this petition and published a notice of docketing in the *Federal Register* on September 22, 2014 (79 FR 56525). This notice included a request for public comments. The public comment period closed on December 8, 2014. The NRC received 19 public comment submissions, 15 of them in support of the petition. The remaining comments either opposed the petition (two comment submissions) or provided other observations on the cyber security rule language (two comment submissions were outside the scope of the PRM). Overall, the comments received do not present additional information to support the petitioner's proposal that the NRC amend its regulations. The enclosed FRN summarizes the comments and provides the NRC staff's response to those comments.

Following docketing of the PRM, the NRC staff established a working group to evaluate the petitioner's request and the public comments received. In 2013, independent of the PRM evaluation, the NRC staff began performing inspections of NRC licensees' 10 CFR 73.54 cyber security programs. By 2016, the NRC staff had completed initial inspections of all NRC licensees' cyber security programs. During this period of time, both, the industry and the NRC staff, gained valuable insights and lessons learned from implementation of the NRC's cyber security requirements. In September 2017 (ADAMS Accession No. ML17179A002), the petitioner was informed by the NRC staff that the PRM would remain open until completion of the assessment of insights and lessons learned from the licensees' implementation of cyber security programs.

In January 2019, the NRC staff began an assessment of the NRC's Power Reactor Cyber Security Program. Based on the results of this assessment, the NRC staff determined there was a need for revisions to existing cyber security guidance documents. The NRC staff has engaged with stakeholders on these potential revisions. In November 2019 (ADAMS Accession No. ML19329C684), the petitioner was informed that the NRC would defer a decision on this PRM for 12 months while it continued to engage with stakeholders on potential revisions to guidance documents. The NRC has determined that existing and ongoing revisions to industry and NRC guidance can effectively address the issues raised by the petitioner in this PRM. For example, the NRC staff reviewed and found acceptable the NEI proposals for risk-informing the identification of critical digital assets (CDAs) for emergency preparedness, balance of plant, important-to-safety and safety-related digital assets (ADAMS Accession Nos. ML20129J981, ML20209A442, and ML20223A256). This new guidance will be risk-informed, will put emphasis on protecting the equipment necessary for maintaining safety, security and emergency preparedness functions, and will significantly reduce the time, resources, and costs associated with protecting these CDAs. Furthermore, the NRC staff plans to capture industry guidance revisions through the normal Regulatory Guide (RG) process in an upcoming revision to RG 5.71, "Cyber Security Programs for Nuclear Facilities." Therefore, for the reasons discussed below and in the enclosed FRN (Enclosure 1), the NRC staff recommends denying PRM-73-18.

DISCUSSION:

Petitioner's Request

The petitioner requested that the NRC amend its power reactor cyber security regulations in 10 CFR 73.54 to make them consistent with the original intent of the rule and clarify that the scope of those regulations only require the protection of those digital assets that, if compromised, can directly cause core damage and spent fuel sabotage, or whose failure would cause a reactor scram.

The NRC staff identified two principal issues in PRM-73-18. First, the petitioner asserts that a rulemaking is needed to clarify the language in 10 CFR 73.54(a) to make it consistent with the original intent of this provision to protect against radiological sabotage by only protecting those digital assets that, if compromised, could directly cause significant core damage or spent fuel sabotage, or whose failure would cause a reactor scram. Second, the petitioner asserts that what it sees as the broad scoping language in 10 CFR 73.54(a)(1) goes considerably beyond the scope of systems and networks necessary to be protected to prevent radiological sabotage, unnecessarily diverting licensee attention from the protection of those digital assets having a direct relationship to radiological sabotage. According to the petitioner, the time, resources and costs of protecting those digital assets not directly related to radiological sabotage from a cyber attack are inconsistent with the intent of the cyber security rule and are not justified.

Summary of Petition Evaluation

The petitioner presented several assertions to support these issues. The NRC staff provides a brief summary and discussion of the petitioner's assertions below. Section III, "Reasons for Denial," of the enclosed FRN discusses the evaluation of the petitioner's assertions in more detail.

Petitioner's Assertion A

In Assertion A, the petitioner states that the scoping language in 10 CFR 73.54(a) was not included in the 2006 proposed rulemaking, "Power Reactor Security Requirements" (71 FR 62664; October 26, 2006) and that this language was added to the 2009 final rulemaking, "Power Reactor Security Requirements," (74 FR 13926; March 27, 2009) without the opportunity for public notice and comment. The petitioner further asserts that the effects of this scoping language were likely not clear when the final rule was issued.

The 2006 proposed rule included a new subsection, 10 CFR 73.55(m)(1), that would have required licensees to have a cyber security program to protect computer systems that, if compromised, would adversely impact safety, security, and emergency preparedness (SSEP).[1] The NRC received several comments on the cyber security requirements in this proposed rule, including a comment that the term "protected computer system" used in 10 CFR 73.55(m)(1)(iii) lacked clarity and should be better defined in the final rule. In response to this comment, the NRC revised the language in 10 CFR 73.55(m)(1), renumbered as 10 CFR 73.54(a) in the 2009 final rule, to provide a more detailed list of the types of computer systems and networks that must be protected from a cyber attack. The language in 10 CFR 73.54(a) of the 2009 final rule clarified but did not substantively change the requirements in the proposed rule. Given these facts, the public was on notice that the NRC intended to apply its new cyber security requirements to the SSEP systems and networks[2] identified in 10 CFR 73.55(m)(1)(iii) of the 2006 proposed rule and included in the 2009 final rule. Therefore, the language in 10 CFR 73.54(a) is consistent with and a logical outgrowth of the language in the proposed rule. Accordingly, the NRC was not required to submit this clarifying language for public notice and comment prior to issuance of the final rule.

[1] While the 2006 proposed rule made reference to "safety, security, and emergency preparedness systems", the 2009 final rule introduced the concept of "safety, security, and emergency preparedness functions." Henceforth, in this paper the staff will use the term "SSEP functions."

[2] While the specific SSEP systems that require protection against a cyber attack vary among licensees, potential systems may include those associated with: (1) shutting down the reactor and maintaining it in a safe shutdown condition; (2) intrusion detection; and, (3) protecting the public in the event of a radiological emergency.

Petitioner's Assertion B

In Assertion B, the petitioner states that the language in 10 CFR 73.54(a)(1) enlarges the scope of digital assets to be protected from cyber attack beyond what the Commission originally intended in the 2006 proposed rule. According to the petitioner, this enlarged scoping language requires the protection of digital assets that cannot cause significant core damage and spent fuel sabotage even if compromised and therefore do not have a nexus to radiological sabotage. According to the petitioner, this creates an inconsistency between the NRC's cyber security requirements and the performance objectives of the physical protection program under 10 CFR 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage" designed to prevent significant core damage and spent fuel sabotage.

The petitioner's Assertion B is based on the assumption that preventing radiological sabotage is limited to protecting only those digital assets that can directly cause significant core damage or spent fuel sabotage if they are compromised. The NRC staff does not agree that only those digital assets that, if compromised, can directly result in radiological sabotage have a nexus to radiological sabotage and are subject to the NRC's cyber security requirements. There is nothing in the language of either the 2006 proposed rule or the 2009 final rule that supports this interpretation. From its inception, the NRC's cyber security requirements were intended to protect computer systems and networks that, if compromised, would have an adverse impact on SSEP functions. As the Commission explained in the Statement of Considerations for the 2006 proposed rule, as computer technology is increasingly integrated into nuclear power plant safety and security systems, the NRC's cyber security requirements minimize potential attack pathways and the consequences of a successful cyber attack. These requirements are part of a defense--in--depth strategy to protect SSEP digital assets that, if compromised, could directly or indirectly result in radiological sabotage at an NRC-licensed nuclear power plant. Additionally, the Commission included EP systems in the cyber security rule because such systems are essential to mitigate the consequences of radiological sabotage. Accordingly, the NRC staff does not agree that the language in 10 CFR 73.54(a)(1) is inconsistent with either the Commission's original intent in promulgating the cyber security rule or the performance objectives in 10 CFR 73.55.

Petitioner's Assertion C

In Assertion C, the petitioner states that the language in 10 CFR 73.54(a)(1) unnecessarily requires licensees to focus on protecting hundreds to thousands of digital assets that have no nexus to radiological sabotage. As a result, the considerable time, resources, and costs needed to protect these assets are not justified.

The NRC staff does not agree that the language in 10 CFR 73.54(a)(1) requires the protection of digital assets that have no nexus to radiological sabotage. The NRC staff recognizes that there may be many digital assets associated with SSEP digital computer and communication systems. The NRC staff does not expect, and the cyber security rule does not require, that all digital assets associated with SSEP functions will necessarily require protection in accordance with the NRC's cyber security rule. For this reason, the language in 10 CFR 73.54 does not mandate that any specific digital asset must be protected. Consistent with 10 CFR 73.54(b)(1), licensees are required to conduct a site-specific analysis of digital computer and communication systems and networks and identify those digital assets that if compromised by a cyber security attack could adversely impact SSEP functions. Only these digital assets, called CDAs, need to be protected against a cyber attack.

The NRC staff recognizes that some licensees, adopting a conservative approach for implementing the NRC's cyber security requirements, included many digital assets within the scope of their cyber security plan that did not have to be protected from a cyber attack. The NRC staff views this as an implementation issue, not an issue with the cyber security rule language. The NRC staff has engaged and continues to engage with stakeholders regarding revisions to industry guidance to assist licensees in better identifying digital assets that fall within the scope of the NRC's cyber security rule. For example, one outgrowth of these engagements is NEI's revisions to NEI 13-10, "Cyber Security Control Assessments," Revision 6, addressing the use of a consequence-based approach for screening CDAs that enables licensees to focus resources on the more consequential digital assets that require protection. The NRC staff is continuing to engage with stakeholders to revise existing guidance to refine the methodology for identifying CDAs.

Petitioner's Assertion D

In Assertion D, the petitioner states that the Commission's policy decision to apply the NRC's cyber security regulations to structures, systems, or components (SSCs) in a nuclear power plant's Balance of Plant expanded the scope of 10 CFR 73.54(a) to include digital assets not strictly necessary to be protected to prevent radiological sabotage.

The NRC staff does not agree with the petitioner's assertion. As the Commission stated in SRM-COMWCO-10-0001 (ADAMS Accession No. ML102940009), it "has determined as a matter of policy that the NRC's cyber security rule at 10 CFR 73.54 should be interpreted to include SSCs in the Balance of Plant that have a nexus to radiological health and safety at NRC-licensed nuclear power plants." In SECY-10-0153, "Cyber Security—Implementation of the Commission's Determination of Systems and Equipment within the Scope of Title 10 of the *Code of Federal Regulations*, Section 73.54," dated November 19, 2010, the NRC staff informed the Commission that it considered SSCs in the Balance of Plant that have a nexus to radiological health and safety to be those that could directly or indirectly affect reactivity of a nuclear power plant, and are therefore within the scope of important-to-safety functions described in 10 CFR 73.54(a)(1) (ADAMS Accession No. ML103490344). Consistent with this, as noted in the NRC's response to petitioner's Assertions B and C, from its inception the NRC's cyber security rule has required the protection of those digital assets associated with SSEP functions that could directly or indirectly cause radiological sabotage. Therefore, the Commission's October 2010 policy determination did not expand the scope of the cyber security rule to include digital assets that do not have a nexus to radiological sabotage.

Petitioner's Assertion E

In Assertion E, the petitioner states that violations of the NRC's cyber security requirements identified during NRC inspections illustrate the problems created by the language in 10 CFR 73.54(a)(1). These violations have typically involved failure to identify CDAs requiring protection under the cyber security rule.

The NRC staff agrees that the NRC's cyber security inspection process has identified violations of NRC cyber security requirements during NRC inspections of licensee cyber security programs. The NRC staff disagrees with the petitioner's assertion that the violations illustrate the problems created by the scoping language in 10 CFR 73.54(a)(1). This scoping language correctly identifies the digital computer and communication systems and networks that the Commission intended licensees to protect against a cyber attack. Rather, the NRC staff has

determined that the violations are the result of issues associated with licensee implementation of the cyber security requirements. As previously noted, the NRC staff is continuing to engage with stakeholders to revise cyber security guidance documents. The NRC staff anticipates that revised guidance will enable licensees to better identify digital assets within the scope of the NRC's cyber security rule.

Other Considerations

Although the focus of PRM-73-18 is specific to the NRC's cyber security regulations for power reactors, in SECY-17-0099, "Proposed Rule—Cyber Security at Fuel Cycle Facilities," dated October 4, 2017 (ADAMS Accession No. ML17018A218), which is currently before the Commission, the NRC staff made a commitment to evaluate the issues raised by the petitioner in PRM-73-18 and determine if they would impact the fuel cycle facilities proposed rule. This proposed rule, if adopted, would require certain fuel cycle facility applicants or licensees to establish, implement, and maintain a cyber security program. As described in more detail in Enclosure 2, "Evaluation of Fuel Cycle Facilities," the NRC staff does not recommend revising the proposed rule for cyber security at fuel cycle facilities in response to any of the issues raised in PRM-73-18.

However, at a public meeting with stakeholders, staff received preliminary information from the fuel cycle industry on the potential resource benefits of adopting a two-step approach to implementing the cyber security plan that would be required by the proposed rule. As discussed further in Enclosure 2, the NRC staff expects to receive additional stakeholder input on this topic during the public comment period associated with the proposed rule.

CONCLUSION:

For the reasons set forth in the FRN attached to this paper as Enclosure 1, the NRC staff has determined that the information presented in PRM-73-18 does not support rulemaking. The NRC's current cyber security requirements are consistent with the NRC's original intent for the cyber security rule, and these requirements continue to provide reasonable assurance of adequate protection of public health and safety, and the common defense and security. Further, the NRC staff has determined that the language 10 CFR 73.54(a) is not overly broad and does not require the protection of digital assets that do not have a nexus to radiological sabotage. Finally, the NRC staff has determined that existing and ongoing revisions to guidance can effectively address the issues raised by the petitioner in this PRM without the need for rulemaking.

RECOMMENDATION:

For the reasons discussed above, the NRC staff recommends that the Commission deny PRM-73-18. The NRC staff recommends the Commission approve publication of the enclosed FRN (Enclosure 1) denying PRM-73-18. This notice provides a detailed response to the petitioner's request and to the public comments that were received. The enclosed letter for signature by the Secretary of the Commission (Enclosure 3) informs the petitioner of the NRC's decision to deny the petition. The NRC staff also will inform the appropriate congressional committees of the NRC's decision.

RESOURCES:

This paper does not address any new commitments or resource implications.

COORDINATION:

The Office of the General Counsel has reviewed this package and has no legal objection to the denial of the petition.

Signed by Doane, Margaret
on 02/02/21

Margaret M. Doane
Executive Director
for Operations

Enclosures:
1. *Federal Register* notice
2. Evaluation of Fuel Cycle Facilities
3. Letter to the Petitioner

SUBJECT: DENIAL OF PETITION FOR RULEMAKING ON PROTECTION OF DIGITAL COMPUTER AND COMMUNICATION SYSTEMS AND NETWORKS DATED: February 02, 2021

ADAMS Accession Nos.: PKG: ML16341B071; **SECY:** ML16237A088; **FRN:** ML20303A245; **Letter to Petitioner:** ML17031A146; **Eval Fuel Cycle Fac:** ML20302A332 ***via email**

OFFICE	NMSS/REFS/RRPB/PM*	QTE*	NMSS/REFS/RRPB/RS*	NMSS/REFS/RASB/RS*
NAME	JLopez	JDougherty	GLappert	DForder
DATE	10/26/2020	10/27/2020	10/30/2020	11/03/2020
OFFICE	NMSS/REFS/RRPB/BC*	NMSS/REFS/RASB/BC*	NSIR/DPCP/CSB/BC*	NRR/DEX/ELTB/BC*
NAME	IBerrios	CBladey	MSampson	JJohnston
DATE	11/06/2020	11/09/2020	11/09/2020	11/06/2020
OFFICE	RES/DE/ICEEB/BC*	NMSS/DFM/FFLB/BC*	NSIR/DPCP/D*	NRR/DEX/D*
NAME	RJenkins	DMarcano	SHelton	EBenner
DATE	11/09/2020	11/09/2020	11/06/2020	11/09/2020
OFFICE	RES/DE/D*	NMSS/DFM/D*	NMSS/REFS/D*	NSIR/D*
NAME	LLund	AKock	JTappert	BHolian (SHelton for)
DATE	11/05/2020	11/09/2020	11/06/2020	11/13/2020
OFFICE	NMSS/D*	OGC*	NRR/D*	EDO
NAME	JLubinski	NSt.Amour	HNieh	MDoane
DATE	11/17/2020	12/09/2020	12/29/2020	02/02/21

OFFICIAL RECORD COPY