[7590-01-P]

NUCLEAR REGULATORY COMMISSION

10 CFR Part 73

[Docket No. PRM-73-18; NRC-2014-0165]

Protection of Digital Computer and Communication Systems and Networks

AGENCY: Nuclear Regulatory Commission.

ACTION: Petition for rulemaking; denial.

SUMMARY: The U.S. Nuclear Regulatory Commission (NRC) is denying a petition for rulemaking (PRM), dated June 12, 2014, submitted by Anthony Pietrangelo on behalf of the Nuclear Energy Institute. 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 can directly cause core damage and spent fuel sabotage, or whose failure would cause a reactor scram. The petition was docketed by the NRC on September 22, 2014, and assigned Docket No. PRM-73-18. The NRC staff has determined that the information presented in PRM-73-18 does not support rulemaking. The NRC has also determined that existing and ongoing revisions to guidance can effectively address the issues raised by the petitioner in this PRM. Therefore, for the reasons discussed in the "Supplementary Information" of this document, the NRC is denying PRM-73-18.

DATES: The docket for the petition for rulemaking, PRM-73-18, is closed on **[INSERT DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**.

ADDRESSES: Please refer to Docket ID NRC-2014-0165 when contacting the NRC about the availability of information for this action. You may obtain publicly-available information related to this action by any of the following methods:

- **Federal Rulemaking Web Site:** Go to https://www.regulations.gov and search for Docket ID NRC-2014-0165. Address questions about NRC dockets to Dawn Forder; telephone: 301-415-3407; e-mail: Dawn.Forder@nrc.gov. For technical questions, contact the individuals listed in the FOR FURTHER INFORMATION CONTACT section of this document.
- **NRC's Agencywide Documents Access and Management System (ADAMS):** You may obtain publicly-available documents online in the ADAMS Public Documents collection at https://www.nrc.gov/reading-rm/adams.html. To begin the search, select "Begin Web-based ADAMS Search." For problems with ADAMS, please contact the NRC's Public Document Room (PDR) reference staff at 1-800-397-4209, 301-415-4737, or by e-mail to pdr.resource@nrc.gov. For the convenience of the reader, the ADAMS accession numbers and instructions about obtaining materials referenced in this notice are provided in the "Availability of Documents" section of this notice. The incoming petition is available in ADAMS under Accession No. ML14184B120.
- **Attention:** The PDR, where you may examine and order copies of public documents, is currently closed. You may submit your request to the PDR via e-mail at PDR.Resource@NRC.gov or call 1-800-397-4209 between 8:00 a.m. and 4:00 p.m. (EST), Monday through Friday, except Federal holidays.

FOR FURTHER INFORMATION CONTACT: Juan Lopez, Office of Nuclear Material Safety and Safeguards; telephone: 301-415-2338; e-mail: Juan.Lopez@nrc.gov; or Ilka Berrios, Office of Nuclear Material Safety and Safeguards; telephone: 301-415-2404; e-mail: Ilka.Berrios@nrc.gov. Both are staff of the U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001.

SUPPLEMENTARY INFORMATION:

TABLE OF CONTENTS:

I. The Petition

Section 2.802 of title 10 of the *Code of Federal Regulations* (10 CFR), "Petition for rulemaking—requirements for filing," provides an opportunity for any person to petition the Commission to issue, amend, or rescind any regulation. On June 12, 2014, the NRC received a PRM from Anthony Pietrangelo on behalf of the Nuclear Energy Institute (NEI or the petitioner). The petitioner requested that the NRC amend its regulations in § 73.54, "Protection of digital computer and communication systems and networks," to clarify the scope of § 73.54(a) to only protect those systems and networks associated with structures, systems, or components (SSCs) that are either necessary to prevent core damage and spent fuel sabotage, or whose failure would cause a reactor scram.

The NRC identified two principal issues in the petition. First, the petitioner asserts that a rulemaking is needed to clarify the language in § 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 § 73.54(a)(1) goes considerably beyond the scope of systems and networks necessary 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 from a cyber attack those digital assets not directly related to preventing radiological sabotage are inconsistent with the intent of the cyber security rule and are not justified. As discussed in the "Reasons for Denial" section of this document, the petitioner presented several assertions to support its petition ~~these issues~~ that the NRC considered in the evaluation the PRM. On September 22, 2014, the NRC published a notice of docketing of PRM-73-18 in the *Federal Register* along with a request for public comment.

II. Background

Following the terrorist attacks of September 11, 2001, the NRC conducted a review of its security requirements to ensure that nuclear power reactors and other licensed facilities could effectively protect against the changing threat environment. Based on this review, the NRC issued a series of security orders imposing new security requirements on nuclear power reactors and other facilities. In NRC Order EA-02-026, "Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants," dated February 25, 2002, the NRC required licensees to address certain cyber security threats at their facilities to protect against a cyber attack. A subsequent order, NRC Order EA-03-086, "Issuance of Order Requiring Compliance with Revised Design Basis

Threat for Operating Power Reactors," dated April 29, 2003, required licensees to address additional cyber attack characteristics.

In 2006, the NRC published in the *Federal Register* a proposed rulemaking, "Power Reactor Security Requirements" (71 FR 62664; October 26, 2006) to amend its existing security requirements and add new security requirements applicable to nuclear power reactors. This proposed rule contained a new § 73.55(m), "Digital computer and communication networks." Section 73.55(m)(1) would have required nuclear power reactor licensees to protect computer systems that, if compromised, would adversely impact safety, security and emergency preparedness (SSEP). Section 73.55(m)(2) would have required licensees to systematically assess and manage cyber risks at their facilities. The NRC received comments on the proposed rule, including comments on § 73.55(m).

After considering all comments, the NRC issued a final rule, "Power Reactor Security Requirements," (74 FR 13926; March 27, 2009). This final rule relocated the cyber security requirements in the proposed rule's § 73.55(m) to a new stand-alone § 73.54 in the final rule. As noted by the Commission in the 2009 final rule Statement of Considerations (SOC), relocating the cyber security requirements into their own stand-alone section was appropriate because the implementation of a cyber security program requires a uniquely independent technical expertise and knowledge that would not necessarily be implemented by security personnel. As further noted, placing the cyber security requirements in a stand-alone section would enable these requirements to be made applicable to other types of facilities in the future, if warranted.

In 2013, the NRC began performing inspections of NRC licensees' 10 CFR 73.54 cyber security programs. By 2016, the NRC had completed initial inspections of all NRC licensees' cyber security programs. During this period of time, both industry and the

NRC gained valuable insights and lessons learned from implementation of the NRC's cyber security requirements.

In January 2019, the Office of Nuclear Security and Incident Response's (NSIR) Cyber Security Branch initiated an assessment of the NRC's cyber security regulations and Power Reactor Cyber Security Program. Its purpose was to identify key areas of improvement that would strengthen the NRC's Power Reactor Cyber Security Program.

The cyber assessment team engaged with external stakeholders to gain additional insights. The Cyber Security Branch in NSIR completed its assessment of the NRC's Power Reactor Cyber Security Program in July 2019. The assessment identified several enhancements to the Power Reactor Cyber Security Program, and the NRC staff developed an action plan to facilitate and prioritize implementation of these enhancements. The enhancements are intended to further risk-inform the NRC's Power Reactor Cyber Security Program. Based on the assessment results, the NRC determined that there was a need to further ~~update~~ revise guidance documents beyond ~~those~~ updates already implemented by industry stakeholders to, among other things, address issues associated with the scoping of critical digital assets (CDAs).

III. Reasons for Denial

The NRC is denying the petition because the petitioner did not present sufficient new information to warrant the requested changes to the NRC's regulations in § 73.54. Specifically, the petitioner did not show that the regulatory language in § 73.54(a) is inconsistent with the original intent of this provision or the cyber security rule and did not show that the regulatory language in § 73.54(a)(1) is overly broad. Furthermore, an assessment of the NRC's cyber security regulations and Power Reactor Cyber Security Program performed by NRC staff as a separate effort from the review of this petition

determined that ~~that~~ existing and ongoing revisions to guidance can effectively address the issues raised by the petitioner in this PRM without the need for rulemaking.

Assertions in the Petition

The assertions made by the petitioner in Section III of PRM-73-18, "Bases for the Action Requested by Petitioner," are summarized in the following paragraphs along with the NRC's responses to those assertions.

Assertion A in Section III of the PRM

In support of its PRM, the petitioner asserts, in part, that the scoping language in § 73.54(a) was not included in the 2006 proposed rule and was added to the 2009 final rule 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.

NRC Response to Assertion A:

The NRC disagrees with the petitioner's Assertion A. The 2006 proposed rule contained a new § 73.55(m) titled "Digital computer and communication networks." Section 73.55(m)(1) would have required licensees to have a cyber security program that would protect computer systems that, if compromised, would adversely impact SSEP. The NRC received several comments on the cyber security requirements in the 2006 proposed rule. This included a comment that the term "protected computer system" used in § 73.55(m)(1)(iii) lacked clarity and should be better defined in the final rule. As the Commission stated in the SOC to the 2009 final rule, in response to a public comment, the NRC revised the language in § 73.55(m)(1), renumbered as § 73.54(a) in the 2009 final rule, to provide a more detailed list of the types of computer systems and

networks requiring protection from a cyber attack consistent with the language in the proposed rule.

The language in § 73.55(m)(1) of the 2006 proposed rule put licensees on notice that they were required to protect computer systems that, if compromised, could adversely affect SSEP. The language in § 73.54(a) of the 2009 final rule, while modifying the 2006 language from "SSEP" to "SSEP functions" to better identify the computer systems and networks requiring protection, did not significantly change any cyber security requirements from the proposed rule to the final rule. The 2009 language is consistent with and a logical outgrowth of the language in the 2006 proposed rule. Accordingly, the NRC was not required to submit this clarifying language for public notice and comment.

Assertion B in Section III of the PRM

The petitioner asserts that one result of the § 73.54(a)(1) language in the 2009 final rule was to enlarge the scope of digital assets to be protected from cyber attack beyond what the Commission originally intended in the 2006 proposed rule. The petitioner further asserts that the § 73.54(a)(1) language requires licensees to implement cyber security controls on hundreds to thousands of digital assets, most of which do not, even if compromised, have a direct relationship to radiological sabotage. According to the petitioner, this creates an inconsistency between the NRC's cyber security requirements and the § 73.55 physical protection program. The petitioner, citing § 73.55(b)(3) and referencing the existing process used to identify target sets, asserts that the performance objectives of the § 73.55 physical protection program must protect against significant core damage and spent fuel sabotage. However, according to the petitioner, because the current language in § 73.54(a)(1) requires the protection of digital assets that cannot, even if compromised, result in significant core damage or spent fuel

sabotage, it is inconsistent with the performance objectives of the § 73.55 physical protection program.

NRC Response to Assertion B:

The NRC disagrees with the petitioner's Assertion B. The petitioner asserts that the language in § 73.54(a)(1) is inconsistent with the cyber security rule's original intent of protecting against the Design Basis Threat (DBT) of radiological sabotage. The petitioner's assertion is predicated on the assumption that protecting against the DBT of radiological sabotage is limited to only protecting that equipment and those digital assets that can directly cause significant core damage or spent fuel sabotage.

The NRC agrees that, consistent with the regulatory language in § 73.54(b)(3) and § 73.55(b)(3), a licensee's cyber security program must protect against significant core damage and spent fuel sabotage. However, the NRC does not agree that protecting against the radiological sabotage DBT only involves protecting those digital assets that can directly cause significant core damage and spent fuel sabotage. Rather, protecting against radiological sabotage also involves protecting those digital assets that could either directly or indirectly cause significant core damage or spent fuel sabotage. Additionally, the NRC included EP systems in the cyber security rule because such systems are essential to mitigate the consequences of radiological sabotage. Accordingly, for the reasons described ~~below~~in this section, the NRC does not agree that the language in § 73.54(a)(1) is inconsistent with either the cyber security rule's original intent of protecting against the DBT of radiological sabotage or inconsistent with the performance objectives of § 73.55.

There is nothing in the language of either the 2006 proposed rule or the 2009 final rule that supports the petitioner's assertion. Section 73.54(a) of the 2009 final rule states the general performance objective that licensees must protect against the DBT as

described in § 73.1. There is no language indicating that protecting against the DBT is limited to protecting only those digital assets that can directly cause significant core damage or spent fuel sabotage. Similarly, Regulatory Guide (RG) 5.71, "Cyber Security Program for Nuclear Facilities," and the other documents cited by the petitioner ~~merely~~ reiterate the general performance objective that licensees must protect against the DBT and prevent significant core damage or spent fuel damage.

The petitioner references the existing process used to identify target sets to support the assertion that the performance objectives of the § 73.55 physical protection program only require protection against significant core damage and spent fuel sabotage. As noted ~~above~~previously, the NRC agrees that a licensee's cyber security program must protect against significant core damage and spent fuel sabotage. The NRC further agrees that the process for developing and identifying target sets defines the set of equipment that must be protected from a physical attack to prevent significant core damage and spent fuel sabotage. The NRC notes that § 73.55(f)(2) requires that licensees consider cyber attacks in the development and identification of target sets. However, the purpose of the cyber security language in § 73.55(f)(2) is to identify a specific type of threat that target sets must be protected from. This language is not intended and should not be used to define the scope of the NRC's cyber security requirements.

As previously noted in the NRC's response to petitioner's Assertion A, § 73.55(m)(1) of the 2006 proposed rule would have required licensees to have a cyber security program that would protect computer systems that, if compromised, would adversely impact SSEP. In the SOC to the 2006 proposed rule, the NRC explained that the cyber security requirements were designed to 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 NRC included EP systems in the cyber security rule because such systems are essential to mitigate the consequences of radiological sabotage.

The NRC made a conscious and deliberate decision to include computer and network systems that could affect SSEP functions in the cyber security rule, even though not all of the equipment and digital assets requiring protection that are associated with those systems can directly cause significant core damage or spent fuel sabotage. The NRC further explained that as computer technology is increasingly integrated into nuclear power plants, many plant safety and security systems rely on this technology to carry out their functions. The NRC intended that digital assets associated with such systems be protected to minimize potential attack pathways that could indirectly or directly result in radiological sabotage. Accordingly, the NRC does not agree with the petitioner's assertion that the original intent of the cyber security requirements in the 2006 proposed rule was limited to protecting only those digital assets that could directly cause significant core damage or spent fuel sabotage. For these reasons, the NRC has determined that the language in § 73.54(a)(1) is consistent with the original intent of the 2006 proposed rule and is consistent with the performance objectives in § 73.55.

Assertion C in Section III of the PRM

The petitioner asserts that the language in § 73.54(a)(1) unnecessarily requires licensees to focus on protecting hundreds to thousands of digital assets at their sites that are, in some way, associated with the SSEP functions identified in § 73.54(a)(1). The petitioner asserts that many of these digital assets have no nexus to radiological sabotage. As a result, the considerable time, resources and costs needed to protect these assets is not justified. The petitioner further asserts that granting the petition will lead to a more efficient use of licensee resources without compromising plant safety or

security.

NRC Response to Assertion C:

The NRC disagrees with the petitioner's assertion that the NRC's cyber security requirements in § 73.54(a)(1) require the protection of hundreds, and in some cases thousands, of digital assets that have no nexus to radiological sabotage. Section 73.54(a)(1) requires that licensees protect ~~from a cyber attack~~ digital computer and communication systems and networks associated with SSEP functions from a cyber attack. The NRC recognizes that these systems may contain hundreds and possibly thousands of digital assets. It is not the NRC's expectation that all digital assets associated with such functions will necessarily require protection in accordance with the NRC's cyber security requirements. Consistent with the requirements in § 73.54(a)(2), only those digital assets that could adversely impact SSEP functions are within the scope of the NRC's cyber security requirements and must be protected against a cyber attack.

Section 73.54(b)(1) requires licensees to conduct an analysis of digital computer and communication systems and networks and identify those digital assets that must be protected against a cyber attack. This requirement reflects the NRC's recognition that licensees are well ~~best~~ situated ~~and able~~ to ~~identify~~ determine the ~~risk~~ safety and security significance of digital systems and assets at their facilities. The NRC issued RG 5.71 to provide guidance to licensees in implementing the NRC's cyber security requirements. Section 3.1.3 of RG 5.71 recognizes that not all digital assets associated with SSEP functions may need to be protected. It sets forth a process for identifying those assets, ~~called~~ referred to as CDAs in the regulatory guide, that must be protected against a cyber attack. CDAs are those digital assets that meet the criteria in § 73.54(a)(2) and, if compromised, could adversely impact SSEP functions.

The petitioner identifies examples of digital assets – specifically fax machines, hand-held calibration devices, radios and pagers, and certain calculators used by licensee staff – that it claims have no nexus to radiological sabotage. The NRC agrees that some digital assets associated with SSEP functions may not need to be protected from cyber attack. Consistent with § 73.54(b)(1), determining whether a specific digital asset, such as a fax machine, calibration device, radio, or the like, has a nexus to radiological sabotage requires a site-specific analysis to determine the ~~risk~~ safety and security significance of the specific asset. The purpose of the analysis is to determine if a specific digital asset must be protected consistent with the criteria in § 73.54(a)(2). That is why neither the NRC's cyber security rule nor RG 5.71 prescribe a list of specific digital assets that must be protected against a cyber attack.

As elaborated in the NRC Response to Assertion B, the NRC does not agree with the petitioner's assertion that only those digital assets that, if compromised, can directly result in radiological sabotage are subject to the NRC's cyber security requirements. Digital assets, the compromise of which may not directly cause significant core damage or spent fuel sabotage, but that could serve as attack pathways that potentially increase the risk of a successful cyber attack if not protected, are within the scope of the NRC's cyber security requirements.

The NRC has been conducting cyber security inspections since 2013 and recently completed a major assessment of the NRC's cyber security requirements. One of the major lessons learned from these inspections and the assessment is that many licensees adopted a conservative approach to identifying digital assets at their facilities that could potentially impact SSEP functions. This resulted in a large number of digital assets being included within the scope of licensees' cyber security programs. As a result of the lessons learned from these inspections and the assessment, the NRC has been and is continuing to engage with stakeholders to revise existing guidance and

refine the methodology for identifying CDAs that fall within the scope of the NRC's cyber security requirements. Based on these interactions, NEI revised NEI 13-10 to include a consequence-based, graded approach for identifying CDAs. The NEI 13-10 guidance enables industry to focus resources on the more significant digital assets. The NRC is continuing to work with stakeholders to identify additional revisions to the guidance for identifying those digital assets that must be protected from a cyber attack. ~~The NRC anticipates that these improvements in guidance may result in a reduction in costs to licensees.~~ For the reasons discussed in this section, the NRC does not agree with the petitioner's assertion that the language in § 73.54(a)(1) requires the protection of digital assets that do not have a nexus to radiological sabotage.

The NRC disagrees with the assertion that the cyber security rule requires the unnecessary expenditure of licensee resources to protect digital assets that have no nexus to radiological sabotage. The NRC issued RG 5.71 in January 2010 to provide guidance to licensees in implementing the NRC's cyber security requirements. It establishes a process for identifying those digital assets, called CDAs, that must be protected against a cyber attack. Some stakeholders have taken a conservative approach to identifying CDAs. The NRC has determined that this is an implementation issue, not an issue with the cyber security rule language. Accordingly, the NRC has been and is continuing to work with industry stakeholders to revise existing guidance and establish new guidance to refine the methodology for identifying CDAs. For these reasons, the NRC does not agree with the petitioner's assertion that the language in § 73.54(a)(1) requires the protection of digital assets that do not have a nexus to radiological sabotage and results in an unjustified burden and costs for licensees.

Assertion D in Section III of the PRM

The petitioner notes that on October 21, 2010, the Commission made a policy

determination to apply the NRC's cyber security rule to SSCs in ~~a nuclear power plant's~~ the ~~B~~balance of ~~P~~plant (BOP) at NRC-licensed nuclear power plants. The petitioner further notes that as a result of this policy determination, SSCs in the BOP were no longer subject to the Federal Energy Regulatory Commission's (FERC) Critical Infrastructure Protection reliability standards. The petitioner states that this policy determination expanded the scope of the cyber security program to include digital assets not strictly necessary to prevent radiological sabotage.

NRC Response to Assertion D:

The NRC agrees with the petitioner that on October 21, 2010, the Commission made a policy determination to apply the NRC's cyber security regulations to SSCs in a nuclear power plant's BOP that have a nexus to radiological health and safety. The petitioner asserts that this policy determination expanded the scope of § 73.54(a) to include digital assets not strictly necessary to be protected to prevent radiological sabotage.

As the petitioner notes, the Commission's October 2010 policy determination applied the NRC's cyber security regulations to BOP digital assets that by themselves, even if compromised, could not directly cause significant core damage or spent fuel sabotage. For the same reasons set forth in the NRC's response to petitioner's Assertions B and C, ~~and as described below,~~ the NRC does not agree with the petitioner's statement that this policy determination resulted in an expansion of the scope of either the 2006 proposed rule or the 2009 final rule.

From its inception, the 2006 proposed cyber security rule would have required licensees to protect those digital assets associated with SSEP that, if compromised, could either directly or indirectly cause radiological sabotage resulting in significant core damage or spent fuel sabotage. 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 BOP ~~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 staff informed the Commission that it considered SSCs in the BOP that have a nexus to radiological health and safety to be those that could, if compromised, directly or indirectly affect reactivity of a nuclear power plant, and are therefore within the scope of important-to-safety functions described in § 73.54(a)(1) ~~(ADAMS Accession No. ML103490344)~~.

Commented [LR1]: Add this document to Section V – Availability of Documents.

To the extent that Assertion D raises issues concerning FERC's jurisdiction at nuclear power plants, the NRC does not have the authority to limit the jurisdiction granted to other agencies by statute.

Assertion E in Section III of the PRM

The petitioner states that, as of March 1, 2014, NRC inspections had identified violations of low safety significance associated with the failure of reactor licensees to identify digital assets needing protection against cyber attacks under § 73.54(a)(1). The petitioner views the violations as an illustration of the problems created by the § 73.54(a)(1) scoping language. The petitioner concludes that although these violations "have little to no safety significance," they have resulted in unnecessary expense and a diversion of licensee resources, as well as conveying to the public "an incorrect impression that the state of cyber security preparedness at those sites is less than adequate."

NRC Response to Assertion E:

The NRC agrees that several violations have been identified during its inspections of licensee cyber security programs at reactor sites. The implementation plan for licensees' cyber security programs, which has eight distinct milestones, was developed to allow a phased approach to full implementation of the cyber security requirements in § 73.54. One of the goals of this phased approach was to allow lessons learned to be applied by licensees prior to full program implementation. The use of this phased approach was intended to identify issues in an iterative way, particularly in regard to digital asset identification. In cases where violations were identified during cyber security inspections of milestones 1 through 7, the NRC performed an evaluation and did not cite the violations if the licensee had made a "good faith" effort to comply with the requirements. Licensees addressed these issues and made corrections to their cyber security programs prior to full program implementation. The identification and resolution of these cyber security issues help ensure that licensees successfully implement an effective cyber security program.

The NRC disagrees with the petitioner's assertion that the violations illustrate problems with the scoping language in § 73.54(a)(1). This scoping language correctly identifies the digital computer and communication systems and networks that the Commission intends licensees to protect against a cyber attack. The language in § 73.54(a)(1) does not identify specific digital assets that must be protected by licensee cyber security programs. It is the responsibility of the licensee to conduct the analysis required by § 73.54(b)(1) and correctly identify those digital assets that, if compromised, could adversely impact SSEP functions. Failure to correctly identify digital assets may result in violations of the NRC's cyber security requirements.

The NRC also disagrees that the violations have conveyed to the public an incorrect impression that the state of cyber security preparedness at reactor sites is less

than adequate. The petitioner provides no evidence that the public has ~~in fact~~ formed such an impression as a result of these violations.

IV. Public Comments on the Petition

The comment period closed on December 8, 2014, and the NRC received 19 comment submissions on the PRM. All of the comment submissions received on this petition are available on https://www.regulations.gov under Docket ID NRC-2014-0165.

Of the 19 comment submissions received, 15 comment submissions supported the petition, two opposed the petition, and two provided other observations on the cyber security rule language. Overall, the comments received do not present additional information to support the petitioner's proposal that the NRC amend its cyber security regulations. The NRC organized the 19 comment submissions into 18 comment categories that are summarized and evaluated in the following paragraphs.

Comment Category 1: Scope of the rule language is too broad.

In support of the PRM, several comment submissions assert that the scope of the existing cyber security requirements in § 73.54 is too broad. They contend that ~~T~~this broad scope has resulted in unnecessary burden on reactor licensees having to maintain hundreds to thousands of digital assets within their cyber security programs. The comment submissions state that most of these digital assets have no nexus to protecting the health and safety of the public. One commenter stated that the high level of protection required by § 73.54 should be focused on the equipment whose compromise could endanger the health and safety of the public. Another commenter stated that the regulations in § 73.54 now allow the NRC to require that licensees classify an excessive number of components as "critical" even though their functions have little or no bearing

on nuclear safety.

NRC Response to Category 1 Comments:

The comments included in Category 1 reiterate assertions made in the petition that the scope of the cyber security rule is too broad. For the reasons set forth in the "Reasons for Denial" section of this document, the NRC does not agree with these comments.

The NRC also disagrees with the commenters' assertion that actions required by § 73.54 are overly burdensome and have no nexus to protecting the health and safety of the public. 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 BOP ~~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 Commission was informed that SSCs in the BOP that have a nexus to radiological health and safety are those that could, if compromised, directly or indirectly affect reactivity of a nuclear power plant, and are therefore within the scope of important-to-safety functions described in § 73.54(a)(1) ~~(ADAMS Accession No. ML103490344)~~.

Consistent with the NRC's cyber security rule, it is the licensee's responsibility to analyze its digital computer and communication systems and networks and identify those digital assets that could adversely impact SSEP functions if compromised by a cyber attack. The NRC agrees with the commenters that some licensees may have conservatively identified certain digital assets that could not adversely impact SSEP functions even if compromised as being within the scope of the NRC's cyber security

rule.

Regulatory Guide (RG) 5.71 contains NRC guidance for complying with the regulations in § 73.54. Licensees may use methods other than those described in RG 5.71 to meet the regulations in § 73.54. The NRC has also engaged 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, as a result of insights gained from these interactions, NEI revised NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," and NEI 13-10, "Cyber Security Control Assessment," to address the application of cyber security controls for CDAs at nuclear power plants. Similarly, NEI revised NEI 13-10, Revision 6, to address scoping issues using a consequence-based approach for screening CDAs. The consequence-based approach in NEI 13-10 enables industry to focus resources on the more consequential digital assets that require protection. The NRC continues to engage with stakeholders to review and revise, as appropriate, relevant cyber security guidance, including guidance on the scoping of CDAs.

Comment Category 2: Implementation costs are significantly higher than those presented in the regulatory analysis for the 2009 rule.

Two comment submissions that support the PRM assert that the costs associated with implementation of the cyber security requirements in § 73.54 are substantially higher than those presented in the NRC's 2009 regulatory analysis (ADAMS Accession No. ML083390372) of these requirements.

NRC Response to Category 2 Comments:

The NRC acknowledges that the costs regarding the implementation of § 73.54 were underestimated in the 2009 regulatory analysis that supported the final rule.

Specifically, the quantity of digital assets identified as CDAs far exceeded the NRC's estimates developed at the time the cyber security rule was finalized. As noted ~~above~~previously, given that many licensees adopted a conservative approach to identifying digital assets at their facilities, the NRC has and is continuing to engage with stakeholders to revise guidance for identifying CDAs. The NRC anticipates that this will reduce the number of identified CDAs and result in a reduction of costs ~~burden~~ to licensees in implementing the NRC's cyber security requirements. As a separate effort, the NRC is reviewing its process for developing cost estimates associated with rulemakings.

Comment Category 3: Unnecessary diversion of licensee resources and attention.

The commenters assert that in determining required cyber security controls, no graded approach is acceptable for use by NRC licensees in complying with the requirements in § 73.54. These commenters assert that the cost of implementing and maintaining these controls contribute no added value, are costly to maintain, and reduce the effectiveness of the digital assets.

One commenter asserts that the current rule language significantly increases costs by: 1) creating a need for vendor processes outside of a well-vetted procurement process; 2) imposing requirements for monitoring and assessment outside of current practices; and 3) failing to accept current maintenance rule analysis of a component's risk significance for exemption from additional treatment. Two commenters assert that the cost of implementing and maintaining the requirements of the rule directly competes with the cost of facility modifications that could improve plant safety, equipment reliability, and reduce the likelihood of an initiating event. Another commenter states that the scope of the existing requirements in § 73.54 introduce significant and unwarranted costs in terms of complying with the requirements in § 73.56, and that these issues

would be resolved by granting the PRM.

Two commenters suggest specific alternatives for refocusing the rule language in § 73.54. One commenter suggests, as an alternative to the petitioner's suggested changes: 1) modifying § 73.54(a)(1)(i) to directly state that only "Target Set and credited security system equipment" need special consideration for preventing the previously established § 73.1 DBT intent of radiological sabotage; and 2) modifying § 73.54(a)(1)(ii) to focus on trips and transients created by cyber attacks initiated by outsiders external to the Protected Area (PA). Another commenter similarly suggested that the NRC refocus the rule language on: 1) high assurance protection for preventing radiological sabotage; 2) preventing plant trips and transients caused by cyber attacks initiated from outside the PA; and 3) preventing accidental initiation of a cyber attack caused by insider action.

NRC Response to Category 3 Comments:

The NRC disagrees that a graded approach is not acceptable for use by licensees in complying with the requirements in § 73.54. A consequence-based, graded assessment process for identifying CDAs and determining the appropriate security controls to be applied to those CDAs may contribute to reducing unnecessary costs to ~~burdens on~~ licensees. Using this graded approach may result in the application of certain minimum cyber security controls to specifically identified CDAs as well as provide a method to assess alternate means of protecting CDAs, for example EP CDAs, from cyber attacks. However, this graded approach will still require that licensees adequately protect CDAs from a cyber attack. For these reasons and the reasons stated in the "Reasons for Denial" section of this document, the NRC disagrees with the assertion that the development of a consequence-based, graded approach for implementing the requirements in § 73.54 contributes no added value, and therefore, results in the unnecessary expenditure of licensee resources.

The NRC also disagrees with the assertion that the application of cyber security controls reduces the effectiveness of digital assets. The commenters did not provide any evidence to support this assertion. The NRC is not aware of any operational experience or data that demonstrates a reduction in effectiveness of digital assets due to the application of cyber security controls to those assets.

The NRC does not agree that the rule language in § 73.54 imposes requirements for monitoring and assessment that are "outside of current practices." The cyber security rule does not require any change to existing licensee monitoring and assessment practices that have already been implemented and does not impose any requirement that licensees develop and implement new monitoring and assessment practices.

The NRC disagrees with the comments regarding limiting the scope of § 73.54 to only target sets and credited security system equipment, and trips and transients created by cyber attacks initiated by outsiders external to the PA. Cyber attacks can adversely affect the performance of SSEP functions of a nuclear facility, which are broader than the functions performed by target sets and security system equipment. As described in RG 5.71, the scope of the cyber security rule goes beyond consideration of cyber attacks initiated by outsiders external to the PA because a defense-in-depth approach requires the licensee to evaluate threats from all possible vectors, including internal and external threats. The NRC further notes that the commenters did not provide a technical basis to support their recommendations.

Certain Category 3 comments are outside the scope of the petition for rulemaking. First, the comment that the requirements in § 73.54 create a need for vendor processes outside of a well-vetted procurement process is outside the scope of the petition. The petition does not discuss the alleged need for additional vendor processes identified in the comment submission. Additionally, the commenter did not

provide any evidence that the NRC's cyber security rule impacts licensee procurement processes. Licensees may procure any computer systems, networks or digital assets that enable them to comply with NRC requirements and are not prohibited by federal law. The cyber security rule requires licensees to ensure that CDAs associated with whatever digital systems the licensee procures are adequately protected from a cyber attack by the application of appropriate security controls. Second, the assertion that the requirements in § 73.54 fail to address the maintenance rule's analysis of a component's risk significance is also outside the scope of the petition. The petition does not discuss the application of the maintenance rule and its discussion of a component's risk significance. Finally, the commenters assertion that the requirements in § 73.54 introduce significant and unwarranted costs in terms of compliance with the access authorization requirements in § 73.56 are also outside the scope of the petition. The petition does not discuss the impact of the cyber security rule on access authorization requirements. Furthermore, the rule does not limit licensees' ability to purchase any digital system that helps it meet the NRC's access authorization requirements~~.~~. The NRC is not aware of any operational experience or data showing that licensees have had significant and unwarranted costs that are unique to compliance with access authorization requirements as a result of the cyber security rule.

Comment Category 4: Issues with process for identification of CDAs.

In support of the PRM, several comment submissions assert that a significant amount of resources are expended on protecting CDAs that have no capability to cause core damage or spent fuel sabotage even if compromised, and that these efforts result in no measurable increase in reactor and spent fuel security. One commenter specifies in this regard that each CDA requires documentation of an assessment ~~of the CDA~~ as configured against the cyber security technical controls in NEI 08-09, Revision 6,

Appendix D, “even if the CDA has no capability to cause core damage or spent fuel sabotage.” Several comment submissions identify CDAs associated with EP communication systems and other equipment as examples of CDAs that should not be included in the scope of the cyber security program. One commenter similarly states that the application of cyber security controls to CDAs is not consistent with other elements of the physical protection program, since cyber security controls are required for systems and equipment that go beyond the systems and equipment necessary to prevent radiological sabotage. One commenter asserts that the resources expended on protecting these CDAs may delay other facility enhancements that would protect more important equipment.

One commenter further states that additional burden is added to protect CDAs when the postulated attack is specific to an active insider with physical CDA access. Two comment submissions cited the Plant Process Computer (PPC) as an example of a system that should not be subject to cyber security requirements.

NRC Response to Category 4 Comments:

These comments reiterate issues raised in the petition; the NRC does not agree with these comments for the reasons stated in the “Reasons for Denial” section of this document.

Regarding the comment that the application of cyber security controls to CDAs for demonstrating compliance with the cyber security requirements in § 73.54 is not consistent with other elements of the physical protection program, the commenter did not provide an example that supports this assertion. Furthermore, the cyber security requirements in § 73.54 are not inconsistent with the physical protection program performance objectives set forth in § 73.55. Specifically, there is no inconsistency as protecting against radiological sabotage is not limited to protecting only those digital

assets the compromise of which can directly cause significant core damage and spent fuel sabotage. Rather, protecting against radiological sabotage involves protecting those digital assets that, if compromised by a cyber attack, could either directly or indirectly cause significant core damage or spent fuel sabotage. As noted ~~above~~previously, the Commission included EP functions within the scope of the cyber security rule because they are essential to mitigate the consequences of radiological sabotage.

Regarding the comment on the need to assess CDAs that have no capability to cause core damage or spent fuel sabotage even if compromised, this essentially repeats assertions made in the petition. The NRC does not agree that protecting against radiological sabotage is limited to protecting only those digital assets that can directly cause significant core damage or spent fuel sabotage if impacted by a cyber attack.

The comments identify the PPC as an example of a system that should not be subject to cyber security requirements. Consistent with § 73.54(b)(1), a licensee must conduct a site-specific analysis to identify those digital assets that meet the criteria of § 73.54(a)(1) and must be protected from a cyber attack. Determining whether or not the PPC should or should not be subject to the NRC's cyber security requirements is dependent upon the outcome of the site-specific analysis.

Comment Category 5: Benefits of granting the petition.

The comment submissions supporting the PRM generally assert that granting the petition would: 1) have an immediate positive impact on overall safety and security while reducing unnecessary burden on reactor licensees; 2) continue to provide defense-in-depth protection for those digital assets having a nexus to radiological safety and security, thereby eliminating the unnecessary diversion of attention and resources expended on protecting digital assets that do not have a nexus to radiological safety and

security; and 3) be consistent with the NRC's original intent to prevent radiological sabotage, in accordance with long-standing physical protection program requirements. Several comment submissions added that if the petition is granted, they would still be able to meet the requirements in § 73.54 to provide high assurance of adequate protection from cyber attacks. Two comment submissions assert that granting the petition would support grid reliability through protection of digital assets capable of causing a reactor trip, and they continue to support having the NRC as the single regulatory authority for cyber security in order to enhance regulatory clarity and implementation efficiency.

NRC Response to Category 5 Comments:

For the reasons set forth in response to petitioner's Assertion B, the NRC disagrees with the commenters' assertion that the current version of the cyber security rule is not consistent with the original intent of the rule.

Additionally, the NRC disagrees with the comments asserting that the petitioner's proposed changes would have an immediate positive impact on overall safety and security while reducing unnecessary burden on reactor licensees. Instead, granting the petition would have the opposite effect as it would increase the risk of SSEP functions being compromised by a cyber attack.

The NRC also disagrees with the commenters' assertions that the petitioner's proposed changes would continue to provide defense-in-depth protection of digital assets (i.e., digital computer and communication systems and networks). The NRC explained in the 2009 SOC that as computer technology is increasingly integrated into nuclear power plants, many plant safety and security systems rely on this technology to carry out their functions. The digital assets associated with these integrated systems must be protected to minimize potential attack pathways and the

consequences of a successful cyber attack. Granting the petition would have the opposite effect as it would remove cyber security protection for such digital assets and decrease defense-in-depth, inconsistent with the rule. For example, the term "defense-in-depth" used in § 73.54(c)(2) requires that a cyber security program be designed to apply and maintain "defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks." In responding to a comment on what became § 73.54(c)(2), the Commission in Section III.D of the 2009 SOC stated that defense-in-depth for digital assets "includes technical and administrative controls that are integrated and used to mitigate threats from identified risks" (74 FR 13934; March 27, 2009).

To the extent that the comment submissions are asserting that the NRC should be the single regulatory authority establishing cyber security requirements ~~as~~ for nuclear power plants, the NRC does not have the authority to limit the jurisdiction granted to other agencies by statute. However, the NRC has worked closely with FERC on matters of mutual interest related to the nation's electric power grid reliability and nuclear power plant safety and security, including but not limited to, coordination of activities related to cyber security at nuclear power plants. By the memorandum of agreement dated September 22, 2015 (ADAMS Accession No. ML15033A181), the NRC and FERC have reached a mutual agreement on how each agency will implement its jurisdiction over cyber security assets at nuclear power plants.

Comment Category 6: Interpretation of "Critical Digital Assets" under the cyber security rule.

One commenter asserts that NRC inspectors have interpreted "critical digital assets" to include backup valve position indicators to which an operator may refer during an abnormal plant condition. The commenter states that if such indicators were affected

by a cyber security event, the required response action could be potentially delayed but would not affect plant safety. The commenter concludes that designating valve position indicators as CDAs "adds hundreds of components to the critical digital asset program" without contributing to plant safety and goes well beyond any reasonable definition of what constitutes a "critical" digital asset.

NRC Response to Category 6 Comments:

The subject of whether any digital asset is a "critical digital asset" is based on a site-specific analysis of digital assets performed by the licensee. RG 5.71, "Cyber Security Program for Nuclear Facilities," NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," and NEI 13-10, "Cyber Security Control Assessment," provide guidance to licensees on the development of licensee cyber security plans that meet NRC requirements, including the process of identifying and implementing appropriate cyber security controls for CDAs.

The NRC is continuing to engage with stakeholders to develop guidance revisions to streamline the process for addressing the application of cyber security controls to CDAs. For example, the NRC has reviewed NEI proposals for risk-informing the identification of CDAs for EP, BOP, important-to-safety and safety-related digital assets (ADAMS Accession Nos. ML20129J981, ML20209A442, and ML20223A256). NEI has stated its intent ~~intends~~ to incorporate these revisions into its guidance documents and to submit them to the NRC for endorsement.

Comment Category 7: Critical Infrastructure Protection standards.

Two comment submissions assert that the evidence required by the NRC and the North American Electric Reliability Corporation Critical Infrastructure Protection standards regarding compliance with cybersecurity requirements should be brought into

closer alignment through rulemaking to reduce the current burden on those utilities that run both nuclear and non-nuclear facilities. The comment submissions further assert that § 73.54 requires utilities to comply with the requirements of multiple regulatory agencies and having to provide different types of evidence to different agencies places unnecessary burdens on the limited number of utility cybersecurity professionals. One of these comment submissions also asserts that a rulemaking should establish clear boundaries of jurisdiction between the NRC and other regulatory agencies**.**

NRC Response to Category 7 Comments:

These comments pertain to issues that were not raised by the petitioner and, therefore, are outside the scope of this PRM. The NRC's cyber security rule is applicable only to NRC power reactor licensees and is not applicable to non-nuclear electric utilities.

Further, to the extent that the comment submissions are asserting that the NRC should establish clear boundaries to limit the jurisdiction of other Federal regulatory agencies, the NRC has no authority to limit the jurisdiction granted to other agencies by statute. However, the NRC has worked closely with FERC on matters of mutual interest related to the nation's electric power grid reliability and nuclear power plant safety and security, including but not limited to coordination of activities related to cyber security, to avoid dual regulation of nuclear power plants. By the memorandum of agreement dated September 22, 2015, the NRC and FERC have reached a mutual agreement of how each agency will implement its jurisdiction over cyber security assets at nuclear power plants.

Comment Category 8: The petition should be denied.

Two comment submissions assert that the petition should be denied. The

commenters assert that granting the petition would roll back cybersecurity regulations essential for nuclear safety. The comment submissions endorse maintaining a high level of cybersecurity protection for both nuclear facilities and communication networks.

NRC Response to Category 8 Comments:

The NRC agrees that the petition should be denied. As discussed in the "Reasons for Denial" section of this document, the existing cyber security regulations in § 73.54 are necessary to ensure adequate protection of digital computer and communication systems and networks associated with SSEP functions and their related support systems.

Comment Category 9: Include PRM-proposed changes in the cyber security event notification rulemaking.

Eleven comment submissions assert that the cyber security event notification rulemaking could provide a ready vehicle for the changes proposed in the petition.

NRC Response to Category 9 Comments:

The Cyber Security Event Notification final rule was published in the *Federal Register* on November 2, 2015 (80 FR 67264). It was a separate action that did not address the issues raised by the petitioner in PRM-73-18. These comments are outside the scope of this PRM.

Comment Category 10: Specific examples of equipment that should not be covered by the cyber security rule.

Nine comment submissions provide examples of equipment that should not be required to be protected by the cyber security rule. Some of the examples the

commenters provide are digital process instruments within BOP systems, wireless control systems associated with plant cranes, non-safety related digital indicators, business computer systems, and cameras, transmitters, and media converters.

NRC Response to Category 10 Comments:

The issue of whether a specific digital asset must be protected from cyber attacks under the regulations in § 73.54 is based on a site-specific analysis made by the licensee. The NRC notes that, to address issues associated with determining if certain equipment should be protected by the cyber security rule, the NRC has found the guidance in NEI 13-10 and NEI 10-04 to be acceptable for use in identifying systems and assets subject to the cyber security rule. NEI 10-04 provides industry with a risk-informed methodology for determining which digital assets should be considered CDAs. NEI 13-10 provides guidance for developing a consequence-based, graded approach to comply with the regulations in § 73.54. This approach provides for the application of certain minimum cyber security controls to specifically identified CDAs, and a method to assess alternate means for protecting certain classes of equipment from cyber attack. Furthermore, the NRC has reviewed NEI proposals for risk-informing the identification of CDAs for EP, BOP, important-to-safety and safety-related digital assets ~~(ADAMS Accession Nos. ML20129J981, ML20209A442, and ML20223A256)~~. NEI has stated its intent ~~intends~~ to incorporate these revisions into its guidance documents and to submit them to the NRC for endorsement.

Commented [LR2]: Add this document to Section V. Availability of Documents

Comment Category 11: Suggested alternatives to granting the petition.

Several comment submissions suggest the NRC should reassess the adequacy of the cyber security rule and should work with external stakeholders to consider other approaches such as a risk-informed, graded approach, or international ISA99 industrial

standards. Several comment submissions provide specific examples of alternate approaches to the cyber security rule. One commenter also asserts that concepts such as redundancy, diversity, and common-cause failures should be reexamined in the context of cyber security.

NRC Response to Category 11 Comments:

In 2019, the NRC performed an assessment of the Power Reactor Cyber Security Program ~~(ADAMS Accession No. ML19175A211)~~. The program assessment identified opportunities to further risk-inform the cyber security guidance in lieu of pursuing changes to the cyber security rule. For example, the NRC has reviewed NEI proposals for risk-informing the identification of CDAs for EP, BOP, important-to-safety and safety-related digital assets ~~(ADAMS Accession Nos. ML20129J981, ML20209A442, and ML20223A256)~~. NEI has stated its intent ~~intends~~ to incorporate these revisions into its guidance documents and to submit them to the NRC for endorsement.

Comment Category 12: NRC should impose additional requirements for cyber security.

One commenter asserts that unintentional or non-malicious cyber incidents are not adequately addressed in NRC guidance documents, and that the NRC should have a requirement to include unintentional cyber incidents. Also, the commenter asserts that engineers and technicians that are experts in instrumentation and control (I&C), electrical engineering, and plant maintenance should be part of the cyber security team, and that the NRC should consider the use of digital I&C and electrical systems for nuclear plant safety applications. The commenter asserts that the training for engineers to be able to identify potential cyber incidents is minimal, and that the current NRC

requirements for cyber security are not conservative when compared to safety requirements.

NRC Response to Category 12 Comments:

The NRC notes that the NRC's cyber security requirements do not distinguish between intentional and unintentional cyber attacks. Licensees are required to protect against any cyber attack that could adversely impact critical digital assets associated SSEP functions. The NRC's existing cyber security regulations in § 73.54 provide high assurance that digital computer and communication systems and networks associated with SSEP functions are protected against a cyber attack. The NRC's cyber security framework also requires that the licensee's cyber security staff have the appropriate training.

Comment Category 13: Examples of cyber security incidents that illustrate need for more requirements.

One commenter who opposes the PRM asserts that the current NRC cyber security requirements need to be strengthened, and that granting the PRM would lessen protection against cyber attacks. The commenter provides examples of cyber security incidents supporting his concern, and further asserts that: 1) the NRC cyber security review of the Oconee I&C upgrade was not adequate, and the NRC should accordingly reassess the adequacy of the cyber security rule because control systems are not adequately protected by the current scope of § 73.54; 2) a comprehensive review is needed to understand the potential system interactions of the different devices in a reactor facility's safety and non-safety systems, and these system vulnerabilities should be covered by § 73.54; 3) air-gapped security measures are not necessarily adequate since it is possible that a well-meaning insider could unintentionally connect infected

portable media to a plant system or component, and the commenter provides examples of how a reactor facility could be compromised using an unintentional insider as a vector for a cyber attack; 4) integrity checking does not offer protection against malicious manipulations until complemented with authenticity checking; and 5) malware has been shown to affect certain cyber vulnerable systems such as human machine interfaces that are used in reactor facilities.

NRC Response to Category 13 Comments:

The NRC agrees that granting the PRM could lessen protection against cyber attacks. For the reasons ~~already~~ set forth in the "Reasons for Denial" section of this document, the NRC has decided to deny the PRM. The commenter is requesting that the NRC take action to ~~modify its cyber protection to~~ strengthen its cyber security requirements to increase protection of digital computer and communication systems and networks at nuclear power plants. The NRC has determined that the current cyber security requirements are robust and provide reasonable assurance that critical digital assets are adequately protected to prevent a cyber attack.

Comment Category 14: Specific Disagreement with petitioner's changes.

Two comment submissions that oppose the PRM assert that the petitioner's proposed changes do not adequately protect safety and security of nuclear power plants, and that the petitioner's proposed changes are not conservative. The comment submissions assert that cyber threats to safety-related and important-to-safety functions can cause, or contribute to, core melt scenarios. The comment submissions also assert that a reduction in cyber security requirements for EP systems is unacceptable because it would not then be possible to meet existing regulations concerning notification of emergency responders if these systems were compromised.

One commenter further asserts that limiting the § 73.54 cybersecurity requirements to the prevention of significant core damage and spent fuel sabotage would not provide effective protection for other safety-critical systems. This commenter also asserts that only the strongest, layered defenses are likely to discourage reconnaissance and attack vector development, and that granting the PRM would 1) eviscerate the NRC's strong cybersecurity regulations and technical guidance; and, 2) exacerbate dependence of nuclear facilities on offsite AC power, therefore producing greater exposure to long-term loss of offsite power risks.

NRC Response to Category 14 Comments:

The NRC generally agrees with these comments. Cyber attacks on safety-related and important-to-safety functions may cause, or contribute to, radiological sabotage (e.g., core melt scenarios). If the provisions in § 73.54(a)(1)(iii) (requiring the protection of digital computer and communication systems and networks associated with EP functions, including offsite communications) were removed as the PRM requests, this would likely hamper a reactor licensee's ability to notify emergency responders in the event that offsite communication systems were compromised in a cyber attack.

The NRC assumes that the commenter's reference to "layered defenses" refers to the concept of defense-in-depth. As discussed in the response to the Category 5 Comments, the existing regulations in § 73.54 reflect a defense-in-depth approach, and the NRC agrees that granting the PRM would not be consistent with maintaining defense-in-depth.

Comment Category 15: RG 5.71 and NEI 08-09 should be reassessed.

Two comment submissions opposing the petition assert that the current regulatory guidance is insufficient. The commenters assert that neither RG 5.71 nor NEI

08-09 addresses cyber threats and vulnerabilities that have been demonstrated to be exploitable, and that the scope of RG 5.71 should be reassessed. One commenter also states that the scope of RG 5.71 should be reassessed to better address control system-specific cyber security issues. The commenters also provide various examples of concerns regarding the current regulatory guidance and specific suggestions for improving this guidance. The commenters assert that the current interpretation of the cyber security rule is increasing plant risk by reducing operational stability. The commenters further assert that configuration changes prescribed by NEI 08-09 and RG 5.71 contribute to uncertainty in the reliability of CDAs. The commenters assert that RG 5.71 should be updated to include consideration of plant risk. One commenter asserts that the existing guidance is too focused on ~~IT~~ information technology and ignores the merits of current protective approaches that are based on traditional I&C Engineering and other license requirements.

NRC Response to Category 15 Comments:

These comments are beyond the scope of the PRM. The petition does not raise the guidance issues identified in the comment submissions. The NRC performs periodic reviews of its guidance documents to determine if they need revision. The results of the most recent periodic review of RG 5.71 can be found under ADAMS Accession No. ML15099A158. The NRC disagrees that the current interpretation of the cyber security rule is increasing plant risk by reducing operational stability. The comment~~s~~ submissions did not provide ~~justification to~~ support for this assertion, and the NRC is not aware of any such reduction in operational stability.

Comment Category 16: Existing plant processes are sufficient to protect most digital equipment.

Two comment submissions that support the PRM assert that while there are thousands of digital assets that are important to the efficient operation of reactor facilities, such assets would be adequately protected by the existing plant controls such as physical protection, network isolation, configuration management, maintenance and testing. One of the comment submissions adds that EP functionality assets, such as communication systems, are typically protected ~~through the use of~~using redundancy and diversity.

NRC Response to Category 16 Comments:

The NRC recognizes that there may be large numbers of digital assets that are important to the efficient operation at a nuclear power plant. These assets may well be protected by existing plant controls. The NRC cyber security requirements do not require the protection of such assets if they cannot adversely impact SSEP functions even if they are compromised. The NRC has determined that CDAs that can adversely impact SSEP functions must be protected from a cyber attack. If a licensee's site-specific analysis can demonstrate that existing plant controls at a given nuclear power plant can protect these CDAs from a cyber attack, then the licensee does not need to apply additional security controls to meet the requirements of the NRC's cyber security rule. If existing plant controls cannot provide such protection, then additional cyber security controls for CDAs would be required.

Comment Category 17: Cyber Security Language was not offered for public comment.

One commenter reiterates the petitioner's assertion that the 2006 proposed rule's scoping language (71 FR 62664; October 26, 2006) was removed and replaced with new text in the 2009 final rule (74 FR 13926; March 27, 2009), asserting that the

practical effect of the new scoping language was likely not clear when the final rule was issued.

NRC Response to Category 17 Comments:

For the reasons stated in the "Reasons for Denial" section of this document, the NRC does not agree with this comment. The clarifying changes made to the scoping language in the 2009 final rule are consistent with and a logical outgrowth of the proposed rule, and the reasons for making these changes were adequately explained in the 2009 SOC.

Comment Category 18: NRC cyber security requirements should be expanded.

One commenter suggested that in order to cover "all digital assets involved in the management of power-block industrial energy," the scope of § 73.54 should be expanded.

NRC Response to Category 18 Comments:

The NRC assumes that in referencing "all digital assets involved in the management of power-block industrial energy" the commenter is referring to digital assets or digital components used to support a reactor facility's on-site power systems. Safety-related digital assets or safety-related digital components interfacing with the facility's on-site power systems are addressed in the safety requirements of 10 CFR part 50 (specifically in appendix A to 10 CFR part 50, general design criterion 17). The commenter does not provide a basis for expanding the scope of § 73.54 to include matters relating to general design criterion 17.

V. Availability of Documents

The documents identified in the following table are available to interested persons through one or more of the following methods, as indicated.

DOCUMENT	DATE	ADAMS ACCESSION NO. OR *FEDERAL REGISTER* CITATION OR WEB SITE
PRM-73-18 – Petition to Amend 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks" submitted by Nuclear Energy Institute (NEI)	June 12, 2014	ML14184B120
Protection of Digital Computer and Communication Systems and Networks; Notice of Docketing and Request for Comment	September 22, 2014	79 FR 56525
PRM-73-18 - Public Comments RE: Protection of Digital Computer and Communication Systems and Networks	August 10, 2020	ML20223A027
SRM-CMWCO-10-0001 – "Regulation of Cyber Security at Nuclear Power Plants"	October 21, 2010	ML102940009
Regulatory Guide 5.71, "Cyber Security Program for Nuclear Facilities"	January 2010	ML090340159
NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6	April 2010	ML101180437
NEI 13-10, "Cyber Security Control Assessment," Revision 6,	August 2017	ML17234A615
Regulatory Analysis and Backfit Analysis; Final Rulemaking: Power Reactor Security Requirements	March 17, 2009	ML083390372
GAO-15-98, NRC Needs to Improve Its Cost Estimates by Incorporating More Best Practices	December 12, 2014	https://www.gao.gov/products/GAO-15-98
SECY-14-0002, "Plan for Updating the U.S. Nuclear Regulatory Commission's Cost-Benefit Guidance"	January 17, 2014	ML13274A495
NUREG/BR-0058, "Regulatory Analysis Guidelines of the U.S. Nuclear Regulatory Commission, Draft Report for Comment," Revision 5	April 2017	ML17100A480
MD 8.2, "Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests"	September 20, 2019	ML18093B087
SECY-20-0008: Draft Final NUREG/BR-0058, Regulatory Analysis Guidelines of the U.S. Nuclear	February 13, 2020	ML19261A277
Memorandum of Agreement between the U.S. Nuclear Regulatory Commission	September 22, 2015	ML15033A181

(NRC) and the Federal Energy Regulatory Commission (FERC)		
SECY-14-0129: Rulemaking: Final Rule: Cyber Security Event Notification (CSEN)	November 20, 2014	ML14136A212
Power Reactor Security Requirements; Final Rule	March 27, 2009	74 FR 13926
Power Reactor Cyber Security Program Assessment	July 12, 2019	ML19175A211
Periodic Review of RG 5.71	April 9, 2015	ML15099A158
Draft Regulatory Guide (DG)-5061, "Cyber Security Program for Nuclear Power Reactor"	August 2018	ML18016A129
Power Reactor Security Requirements; Proposed Rule	October 26, 2006	71 FR 62664
Cyber Security Event Notifications; Final Rule	November 2, 2015	80 FR 67265
Memorandum of Understanding Between the U.S. Nuclear Regulatory Commission and the North American Electric Reliability Corporation	December 17, 2019	ML093510905
EA-02-026, Issuance of Order for Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants	February 25, 2002	ML020510635
EA-03-086, "Issuance of Order Requiring Compliance with Revised Design Basis Threat for Operating Power Reactors"	April 29, 2003	ML030740002

VI. Conclusion

For the reasons discussed in this document, the NRC finds that the petitioner did not present sufficient new information to warrant the requested changes in PRM-73-18. 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 has determined that the language in § 73.54(a) is not overly broad. Finally, the NRC has determined that existing and ongoing revisions to guidance can effectively address the other issues raised by the petitioner in this PRM without the need for rulemaking. Accordingly, the NRC is denying the PRM-73-18 ~~for~~

~~the reasons discussed in this document~~.

Dated Month XX, 20XX.

For the Nuclear Regulatory Commission.
Annette L. Vietti-Cook,
Secretary of the Commission.