ANTHONY R. PIETRANGELO
Senior Vice President and
Chief Nuclear Officer

1201 F Street, NW, Suite 1100
Washington, DC 20004
P: 202.739.8081
arp@nei.org
nei.org

NUCLEAR ENERGY INSTITUTE

June 12, 2014

Ms. Annette L. Vietti-Cook
Secretary
Attn: Rulemaking and Adjudications Staff
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Petition to Amend 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks"

Project Number: 689

Dear Ms. Vietti-Cook:

On behalf of its members and pursuant to 10 CFR 2.802, the Nuclear Energy Institute, Inc. (NEI)[1] submits the enclosed petition to amend 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks." The purpose of this petition is to request that the NRC revise certain cyber security language in 10 CFR 73.54(a) to ensure it is consistent with the NRC's original intent, less burdensome for NRC licensees, and adequately protective of the public health and safety and common defense and security. NEI requests that the NRC promptly initiate rulemaking to resolve this matter.

On or before December 31, 2012, NRC power reactor licensees completed implementation of the elements of the cyber security program designed to mitigate the most likely attack pathways, and assessed and implemented protective measures for the most risk-significant plant components. Industry experience gained from implementing 10 CFR 73.54 over the last five years has identified a problem stemming from the

[1] NEI is the organization responsible for establishing unified nuclear industry policy on matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include all entities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect/engineering firms, fuel fabrication facilities, nuclear material licensees, and other organizations and individuals involved in the nuclear energy industry.

broad scoping language in 10 CFR 73.54. This language does not accurately reflect the intended objective of the cyber security rule which is to prevent radiological sabotage. Specifically, the scope of Section 73.54(a)(1) has resulted in reactor licensees having to implement cyber security controls on hundreds to thousands of digital assets, most of which have no direct relationship to radiological sabotage. This rulemaking petition is intended to obtain greater alignment between the scoping language in 10 CFR 73.54(a)(1) and the agency's intended objective to prevent radiological sabotage. In doing so, the rulemaking should substantially enhance regulatory clarity and implementation efficiency. Further, revising the scoping language will also eliminate the unnecessary diversion of NRC licensee attention and resources from protection of assets that have a nexus to radiological safety and security.

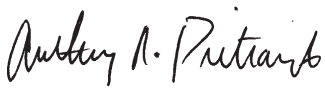
The current rule language is inconsistent with the NRC's Principles of Good Regulation, which include "Efficiency." NRC describes efficient regulation as including the following: "Regulatory activities should be consistent with the degree of risk reduction they achieve. Where several effective alternatives are available, the option which minimizes the use of resources should be adopted. Regulatory decisions should be made without undue delay." This petition for rulemaking is the option that best promotes regulatory efficiency, as well as other principles of good regulation such as clarity and reliability. Regarding the need for clarity, NRC states, "Regulations should be coherent, logical, and practical. There should be a clear nexus between regulations and agency goals and objectives whether explicitly or implicitly stated. Agency positions should be readily understood and easily applied."

Further, this petition promotes NEI's ongoing efforts to facilitate the agency's reduction of the cumulative impacts of regulation. The petition proposes a simple change to 10 CFR 73.54 that relies on existing, well understood regulatory language to more precisely align the scope of the cyber security rule with the underlying agency objective of preventing radiological sabotage. As the proposed language is easily understood, the revised regulatory requirements can be easily adopted by NRC licensed power reactors – resulting in a substantial reduction in burden while maintaining adequate protection against cyber attacks.

We believe the change proposed in this petition is the single most important near-term regulatory improvement that can be made in the area of cyber security. It would provide the largest benefit to regulatory clarity and stability by assuring that licensees have identified for protection those assets which, if compromised by a cyber attack, would be inimical to the health and safety of the public.

If you have any questions concerning this petition, please contact William Gross at (202) 739-8123; wrg@nei.org or me.

Sincerely,



Anthony R. Pietrangelo

Attachment

c: The Honorable Allison M. Macfarlane, Chairman, NRC
The Honorable Kristine L. Svinicki, Commissioner, NRC
The Honorable William C. Ostendorff, Commissioner, NRC
The Honorable William D. Magwood, IV, Commissioner, NRC
The Honorable George Apostolakis, Commissioner, NRC
Mr. Mark A. Satorius, EDO, NRC
Mr. James T. Wiggins, NSIR, NRC
Mr. Barry C. Westreich, NSIR/CSD, NRC
NRC Document Control Desk

Petition to Amend 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks"

Before the
UNITED STATES NUCLEAR REGULATORY COMMISSION
Rockville, Maryland

In the Matter of a Proposed Rulemaking to Amend 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks"

Docket No. _____

PETITION FOR RULEMAKING BY THE NUCLEAR ENERGY INSTITUTE

I. OVERVIEW

This petition for rulemaking is submitted pursuant to 10 CFR 2.802 by the Nuclear Energy Institute, Inc. (NEI) on behalf of its members.[1] Petitioner NEI requests that the U.S. Nuclear Regulatory Commission (NRC), following public notice and opportunity for comment, promptly initiate a rulemaking to amend certain cyber security requirements in 10 CFR 73.54(a). As demonstrated herein, a rulemaking is needed to clarify the scope of Section 73.54(a) to make it fully consistent with the original intent of this provision to prevent radiological sabotage, specifically, significant core damage and spent fuel sabotage.[2]

Industry experience gained from implementing Section 73.54 over the last five years has identified a problem stemming from the overbroad scoping language in 10 CFR 73.54(a)(1), which describes those digital computer and communication systems and networks at commercial nuclear power plants that must be protected against cyber attack. As promulgated, Section 73.54(a)(1) goes considerably beyond the scope of systems and equipment necessary to prevent radiological sabotage.

Power reactor licensees are required to establish and maintain a physical protection program to protect against the design basis threat of radiological sabotage as described in 10 CFR

[1] NEI is the organization responsible for establishing unified nuclear industry policy on matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include all utilities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect/engineering firms, fuel fabrication facilities, materials licensees, and other organizations and individuals involved in the nuclear energy industry.

[2] Consistent with the requirements of 10 CFR 2.802, this Petition sets forth a clear and concise statement of the grounds for the action requested, NEI's interest in the action requested, the regulations that NEI seeks to have amended, the legal and regulatory bases for our request, NEI's recommended solution to the problem, and proposed regulatory language revising 10 CFR 73.54(a)(1).

73.1. In accordance with the definition of radiological sabotage in 10 CFR 73.2, licensees are required to protect against any deliberate act which could directly or indirectly endanger the public health and safety by exposure to radiation. To accomplish this, the physical protection program for NRC-licensed power reactors is designed to prevent significant core damage and spent fuel sabotage. The design basis threat described in 10 CFR 73.1 includes five attributes: a physical assault; an internal threat; a land vehicle bomb assault; a waterborne vehicle bomb assault; and a cyber attack. In order to prevent radiological sabotage, licensees have well-established programs to identify the set of personnel, systems, and equipment that must be protected against the design basis threat in order to prevent significant core damage and spent fuel sabotage.

The NRC's cyber security rule, codified in 10 CFR 73.54, provides the programmatic requirements to defend against the design basis threat of radiological sabotage through a cyber attack. 10 CFR 73.54(a)(1) contains scoping language that requires licensees to protect certain digital assets against cyber attack even though those digital assets, if compromised, would not adversely impact the systems and equipment necessary to prevent significant core damage and spent fuel sabotage. This language requires NRC licensees to protect one set of systems and equipment against the effects of four of the attributes of the design basis threat (physical assault; internal threat; land vehicle bomb assault; waterborne vehicle bomb assault), and a substantially broader set of assets against a the fifth design basis threat attribute, cyber attack. Further, this regulatory language is inconsistent with both the agency's intent in promulgating the cyber security requirements and the NRC's programmatic requirements to defend against other attributes of the radiological sabotage design basis threat.

Additionally, the language of Section 73.54(a)(1) unnecessarily diverts NRC licensee attention and resources from the protection of assets that have a nexus to radiological safety. This provision burdens NRC reactor licensees without providing a commensurate enhancement in the protection of the public health and safety, or plant security. For digital assets that do not reasonably require protection against radiological sabotage, the considerable time, resources, and cost needed to protect them against cyber attack is unjustified. In this regard, the current cyber security provision fails to comply with the Commission's Principles of Good Regulation.

The industry has brought to the attention of the NRC staff the significant problems created by the current scoping language in Section 73.54(a), and has determined that revisions to NRC regulations are needed to address this problem.[3] More importantly, implementing the revisions proposed herein will not adversely affect NRC licensees' ability to ensure that public health, safety and security are being adequately protected.

[3] After evaluating several alternatives to a petition for rulemaking, we concluded that rulemaking offers the best process for resolving this issue. For example, revising NRC Regulatory Guide 5.71 and NEI 10-04, "Identifying Systems and Assets Subject to the Cyber Security Rule," Revision 2, without requesting rulemaking would not effectively enhance regulatory stability or assure long-term consistency in the same manner as an amended regulation. Similarly, we concluded that requesting NRC development of a generic communication, e.g., a Regulatory Issue Summary or Generic Letter, without a related rulemaking would not be optimal.

This Petition identifies revisions to Section 73.54(a)(1) that would more precisely align the rule language with the agency's intent to prevent radiological sabotage by protecting against cyber attacks those digital computer and communication systems and networks associated with the systems and equipment necessary to prevent significant core damage and spent fuel sabotage. These amendments, if implemented, will make Section 73.54(a) consistent with programmatic requirements to defend against other attributes of the radiological sabotage design basis threat. Such revisions will also more appropriately focus licensees' limited implementation resources on protecting those assets that have a nexus to ensuring the health and safety of the public, and help achieve needed regulatory clarity.

Under the current cyber security regulations NRC reactor licensees must perform cyber security assessments on thousands of digital assets before their committed full program implementation date for the cyber security program. The industry and the NRC have taken action to appropriately focus these assessments, culminating in the February 2014 NRC endorsement of the industry's NEI 13-10, "Cyber Security Control Assessments." However, merely refocusing the assessment cannot alleviate the underlying problem with the cyber security rule. Rulemaking action is needed to ensure licensees focus their resources on protecting assets with a nexus to radiological safety and security. In turn, a revision to Section 73.54 will significantly reduce the regulatory uncertainty that underlies the dozens of enforcement violations of this provision. Those violations speak to the lack of a consistent understanding of this provision. Further, the changes proposed in this Petition do not lengthen the time necessary for licensees to implement their cyber security programs. In fact, amending Section 73.54 as requested may in fact reduce the time needed to reach full implementation.

The set of digital assets currently identified by licensees under Section 73.54(a) includes those assets necessary to prevent radiological sabotage. Accordingly, NEI requests that, once promulgated, the amendments to Section 73.54(a) become effective immediately after issuance of the final rule. In this regard, NEI understands that the NRC staff has in some cases exercised enforcement discretion during the inspection of the interim cyber security milestones for licensees that demonstrate a good faith interpretation of requirements. NEI asks that, until rulemaking is completed and a final rule is issued, NRC continue to grant enforcement discretion in connection with 10 CFR 73.54(a).

To prevent radiological sabotage, the set of systems and equipment protected against cyber attack should be the same set of systems and equipment that are protected against the other attributes of the design basis threat. Licensees should protect against the effects of the cyber attack design basis threat those digital computer and communication systems and networks associated with systems and equipment necessary to prevent significant core damage and spent fuel sabotage.

To ensure that the full benefits of improved regulatory efficiency and effectiveness are achieved through the proposed rulemaking, we recognize that accompanying implementation guidance must be developed. Consistent with the Commission's direction in SRM-SECY-11-0032, "Consideration of the Cumulative Effects of Regulation in the Rulemaking Process," if this Petition is accepted NEI commits to develop guidance, which we will submit for NRC endorsement in conjunction with the proposed rulemaking.

II. PETITIONER'S INTEREST IN THE ACTION REQUESTED

As required by 10 CFR 2.802, NEI has a clear and substantial interest in the rulemaking action requested. As the policy organization for the commercial nuclear industry, NEI is responsible for establishing a unified industry position on matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include entities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, architect/engineering firms, fuel fabrication facilities and other materials licensees, and other organizations and entities involved in the nuclear energy industry. In particular, NEI's members operate numerous power reactor facilities licensed by the NRC through 10 CFR Part 50 and Part 52. As such, these NEI member companies are subject to NRC regulation under 10 CFR Part 73.

NEI is responsible for coordinating industry activities and projects on generic operational, technical and regulatory issues affecting the activities of NRC-licensed power reactors. NEI member companies are specifically affected by the cyber security regulations that are the subject of this Petition. To support licensee implementation of the NRC's cyber security requirements, NEI, with participation from licensees, developed a template for the cyber security plan that is required by 10 CFR 73.54(e); a template for the implementation schedule required by the undesignated paragraph preceding 10 CFR 73.54; and other guidance documents intended to support uniform implementation of the cyber security requirements. NEI continues to engage with the power reactor licensee community to identify and develop guidance to support implementation of an effective cyber security program. In its role, NEI provides a principal interface between power reactor licensees and the NRC on matters of policy, including cyber security-related policy. For all of these reasons, NEI is keenly interested in facilitating NRC's consideration of the proposed revision to 10 CFR 73.54(a).

III. BASES FOR THE ACTION REQUESTED BY PETITIONER

As required by 10 CFR 2.802, this Petition explains the bases for the requested rulemaking action. The cyber security rule at 10 CFR 73.54 provides the programmatic requirements to defend against the design basis threat of radiological sabotage cyber attack. However, as discussed more fully in Section III.C, below, the broad language in Section 73.54(a)(1) has resulted in scoping in digital assets that have no nexus to preventing radiological sabotage.

The proposed amendments to 10 CFR 73.54(a)(1) are designed to accomplish several purposes, including the following:

- Protect the public health and safety and the common defense and security by preventing radiological sabotage. This is accomplished by continuing to require licensees to protect against cyber attack the digital computer and communication systems and networks associated with the systems and equipment necessary to prevent significant core damage and spent fuel sabotage.

- Enhance regulatory clarity.

- Eliminate unnecessary compliance burdens for NRC licensees that do not produce a commensurate enhancement of plant safety and security.

A. Regulatory Background Supports the Need to Amend Section 73.54(a)(1)

Power Reactor Licensee Security Rulemaking

The NRC issued a proposed rule on October 26, 2006, amending previous security provisions for NRC reactor licensees and adding new ones, including more detailed programmatic requirements to defend against the design basis threat of radiological sabotage cyber attack. 71 Fed Reg. 62664 *et seq*. (Oct. 26, 2006). The proposed rule points out that the cyber security rule is intended to "build on the requirements imposed by the February 2002 [NRC] Order." *Id*. at 62667.

The Design Basis Threat (DBT) Rulemaking

In another security-related rulemaking, NRC issued a final rule imposing on the industry security requirements similar to those previously imposed by the Commission's April 29, 2003 DBT Orders. See 72 Fed. Reg. 12705 *et seq*. (Mar. 19, 2007). This rulemaking revised the design basis threat requirements in 10 CFR 73.1 to explicitly include a cyber attack as an attribute of the design basis threats of radiological sabotage and theft or diversion of formula quantities of strategic special nuclear material. See 72 Fed. Reg. 12705, at 12707-08, 12722-24, 12727. The NRC rule described the design basis threat of cyber attack as: "The capability to exploit site computer and communications system vulnerabilities to modify or destroy data and programming code, deny access to systems, and prevent the operation of the computer system and the equipment it controls." 72 Fed. Reg. 12723, 12724.

In the reactor licensee security rulemaking, NRC issued final amendments to the power reactor security requirements in March 2009. The proposed cyber security provision was removed from Section 73.55 and promulgated under a new section, 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks." See 74 Fed. Reg. 13926 *et seq*. The cyber security rule requires licensees to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks up to and including the design basis threat of radiological sabotage cyber attack as established by 10 CFR 73.1(a)(1)(v). 74 Fed. Reg. at 13927.

When the final rule was issued, the cyber security requirements were placed in a stand-alone section. The Commission stated in the discussion accompanying the final rule that it moved the cyber security provision from Section 73.55(m) to a new Section 73.54 "because cyber security is not implemented by physical security personnel." The Supplementary Information accompanying the rule also stated that the cyber security provisions were separated out "to enable the cyber security requirements to be made applicable to other types of facilities and applications through future rulemakings." See 74 Fed. Reg. at 13928, 13933.

When the cyber security provision was relocated to another regulation, the rule's original scoping language was removed and replaced with new text. The scoping language in the final rule promulgating 10 CFR 73.54(a) requires, in part (emphasis added):

> (a) Each licensee subject to the requirements of this section shall provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in § 73.1.

(1) The licensee shall protect digital computer and communication systems and networks associated with:
   (i) Safety-related and important-to-safety functions;
   (ii) Security functions;
   (iii) Emergency preparedness functions, including offsite communications; and
   (iv) Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

Notably, this scoping language was added to the final rule and was not included in the proposed rule. Therefore, there was no opportunity for stakeholder comment on this aspect of the final rule. The practical effect of the new, more expansively worded scoping language relating to protection of digital assets against cyber attack was likely not clear when the final rule was issued.

B. The Current Scoping Language Does Not Reflect the Original NRC Intent in Promulgating the Cyber Security Rule

Moving the cyber security provision into a new stand-alone Section 73.54(a)(1) and adding different scoping language to that provision has greatly complicated the identification of assets that must be protected. One result of the 2009 final rule was to enlarge the scope of equipment to be protected. Another result was to create an inconsistency between the cyber security requirements and the overall physical protection program design requirement to prevent significant core damage and spent fuel sabotage. This is counterproductive because the cyber security program is an integrated component of the physical protection program. The existing cyber security rule requires NRC licensees to protect any digital asset associated with the broad functions in 10 CFR 73.54(a)(1) against the design basis threat of radiological sabotage through cyber attack. Given the rule language, this action must be taken without considering the nexus between the consequences of a cyber attack on those assets and the potential for radiological sabotage.[4]

In sum, the language in 10 CFR 73.54(a)(1) has created inconsistency between the intended objective of the cyber security rule (to prevent radiological sabotage) and the set of assets licensees have identified for protection against cyber attack.

Evidence that the cyber security rule was intended to maintain the intent to protect against cyber attacks systems and equipment necessary to prevent radiological sabotage appears in several NRC documents. For example, Section C.3.1.3 of the Regulatory Position supporting RG 5.71 states, "To the extent that these systems are associated with SSEP [Safety, Security, and Emergency Preparedness] functions, a compromise of these plant systems

[4] NRC Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities," and NEI 10-04, "Identifying Systems and Assets Subject to the Cyber Security Rule," Revision 2 (endorsed), provide guidance for identifying assets that must be protected against cyber attacks. These guidance documents are based on the very broad scoping language in 10 CFR 73.54(a)(1) and do not provide for consideration of the nexus between these digital assets and the consequence of radiological sabotage.

could result in radiological sabotage (i.e. significant core damage) and therefore has the potential to adversely impact the public health and safety." As another example, in a January 15, 2010 letter to Melvin Leach, [ADAMS Accession Number ML100130359], Richard Correia, Director of the Division of Security Policy, Office of Nuclear Security and Incident Response, wrote, "In addition, the DSP staff notes that the primary intent of the 10 CFR 73.54 regulations is to ensure that licensees provide adequate protection for digital computer and communication systems and networks whose failure or compromise from cyber attack could lead to a radiological sabotage event." In COMWCO-10-001, dated September 14, 2010, Commissioner William Ostendorff wrote: "In March 2009, the Commission issued a final rule, 10 C.F.R. § 73.54, which set forth cyber security requirements applicable to NPP licensees. This regulation was intended to apply to digital SSCs within an NPP that, if compromised, could result in radiological sabotage." These references support NEI's view that the rule is intended to prevent radiological sabotage, and that the broad scoping language added to the final rule is not intended to expand beyond protecting those assets necessary to prevent radiological sabotage.

Protecting the systems and equipment necessary to prevent radiological sabotage against cyber attack is consistent with the overall performance objectives in 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage." 10 CFR 73.55(b), "General Performance Objective and Requirements," outlines the general performance objective and design requirements of NRC licensees' physical protection program, of which the cyber security program is an integrated component. 10 CFR 73.55(b)(2) requires that the physical protection program must protect against the design basis threat of radiological sabotage. 10 CFR 73.54(b)(3) requires that the physical protection program must be designed to prevent significant core damage and spent fuel sabotage. The prevention of significant core damage and spent fuel sabotage is the established criteria to measure a licensee's performance to protect against radiological sabotage.

NRC licensees have well-established practices for identifying the set of personnel, equipment, and systems necessary to prevent significant core damage and spent fuel sabotage. This is exemplified by the industry's longstanding practices for the development, identification, and protection of target sets. Target sets include, in part, the combination of equipment or operator actions which, if all are prevented from performing their intended safety function or prevented from being accomplished, would likely result in significant core damage barring extraordinary action by plant operators.

10 CFR 73.55 provides programmatic requirements to defend against other attributes of the radiological sabotage design basis threat, and includes language that we propose be used to revise 10 CFR 73.54 to achieve the needed clarity. For example, a land vehicle bomb assault is included in 10 CFR 73.1(a)(1)(iii) as an attribute of the radiological sabotage design basis threat. To defend against the land vehicle bomb assault, 10 CFR 73.55(e)(10)(i)(A) requires licensees to "design, construct, install, and maintain a vehicle barrier system, to include passive and active barriers, at a stand-off distance adequate <u>to protect personnel, equipment, and systems necessary to prevent significant core damage and spent fuel sabotage</u> against the effects of the design basis threat of radiological sabotage land vehicle bomb assault," (emphasis added).

In order to prevent radiological sabotage, the set of systems and equipment protected against cyber attack should be the same set of systems and equipment that are protected against the other attributes of the design basis threat. Licensees should protect against the

effects of the cyber attack design basis threat those digital computer and communication systems and networks associated with systems and equipment necessary to prevent significant core damage and spent fuel sabotage.

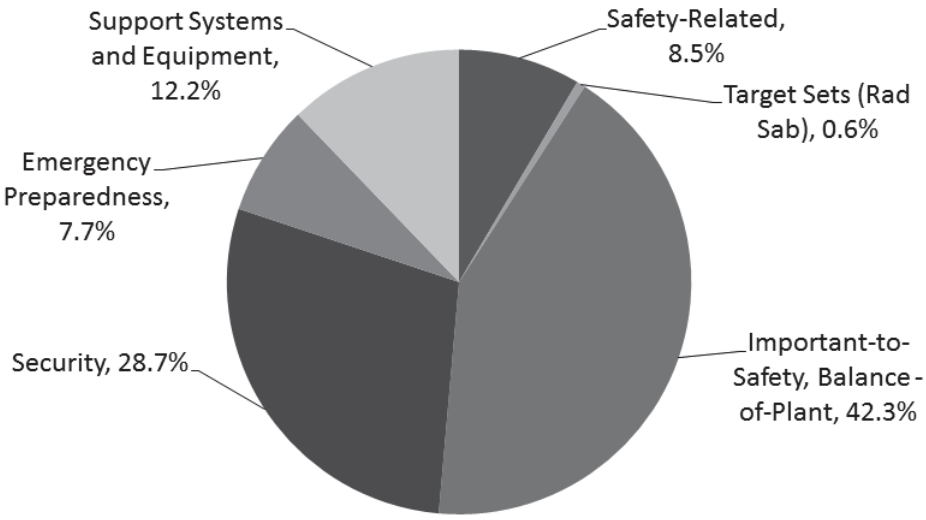
C. Amending Section 73.54(a)(1) Will Promote More Efficient Use of Resources While Continuing to Provide High Assurance of Protection against Cyber Attack

Since the 2009 security rule was promulgated, the inconsistency between the scoping language of Section 73.54(a)(1) and the more focused objective of the cyber security rule has unnecessarily diverted NRC reactor licensees' attention toward protecting non-risk-significant assets. For digital assets that have no nexus to preventing radiological sabotage, the considerable time, resources, and cost needed to protect them against cyber attack is not justified, and does not increase protection of the public health and safety and/or facility security.

The current language in Section 73.54(a)(1) also has resulted in power reactor licensees identifying hundreds to thousands of digital assets at their sites as requiring protection against cyber attack. Indeed, in some cases NRC licensees have identified a majority of both installed and non-installed digital equipment used at their facilities as being included for protection, principally because these assets are, in some more or less attenuated way, associated with the range of functions identified in 10 CFR 73.54(a)(1). Examples of assets that have been identified as requiring protection against cyber attack and that simply have no nexus to preventing radiological sabotage include: individual digital indicators on non-safety-related equipment, fax machines, hand-held calibration devices, radios and pagers, and calculators used by emergency preparedness personnel.

The industry addressed this concern on February 19, 2014, during a closed briefing on cyber security with the Commission of the NRC. During that engagement, NEI provided results of an industry benchmarking exercise, illustrated in Figure 1 below, demonstrating that *less than ten percent* of identified digital assets were associated with safety-related functions, with an even smaller percentage (*less than one percent*) having a nexus to radiological sabotage.

Figure 1: Digital Assets By Percentages



Also during the February 19 Commission briefing, two licensees provided a detailed description of their current expenditures required to comply with the existing cyber security requirements. Both licensees indicated that the current and projected full program implementation costs *substantially exceed* the cost estimates provided in the regulatory analysis for the rulemaking included in Enclosure 2 to SECY-08-0099 (July 9, 2008). A key driver for the costliness of compliance is the large number of non-safety-related digital assets identified for protection against cyber attack.

There are also other related NRC rules that are inappropriate and unreasonably burdensome when applied to the requirement to protect digital assets with no nexus to radiological sabotage. For example, 10 CFR 73.56(i)(1)(v)(B)(4) requires enhanced scrutiny of personnel performing certain job functions.

> (B) For individuals who perform one or more of the job functions described in this paragraph, the trustworthiness and reliability determination must be based on a criminal history update and credit history re-evaluation within three years of the date on which these elements were last completed, or more frequently, based on job assignment as determined by the licensee or applicant, and a psychological re-assessment within 5 years of the date on which this element was last completed:
> (4) Individuals who have access, extensive knowledge, or administrative control over plant digital computer and communication systems and networks as identified in § 73.54, including—
> (i) Plant network systems administrators;
> (ii) IT personnel who are responsible for securing plant networks.

The large number of digital assets identified for protection under Section 73.54(a) unnecessarily increases the population of individuals subject to this increased scrutiny.

The revisions proposed in this Petition would promote a more efficient use of NRC licensees' resources by focusing implementation on protecting against cyber attack the systems and equipment necessary to prevent radiological sabotage. And as discussed elsewhere in the petition, revising Section 73.54(a) as proposed would in no way compromise plant safety or security. Licensees have a long history of addressing the cyber threat, and have a vested interest in implementing cyber security programs at their facilities. Digital assets that would not be subject to the requirements of 10 CFR 73.54 would be protected consistent with prudent business practices.

D. The Benefits of a Single Regulatory Authority for Cyber Security Will Be Retained if this Petition Is Granted

The scope of assets identified as requiring protection in accordance with Section 73.54(a) has also been affected by the fact that, after issuance of the cyber security rule, the NRC expanded the scope of that rule to include structures, systems, and components (SSCs) in the Balance-of-Plant (BOP). See COMWCO-10-001, "Regulation of Cyber Security at Nuclear Power Plants" (Sept. 14, 2010).[5] This expansion has the effect of protecting against cyber attacks BOP SSCs that would, if not included within the scope of the NRC's cyber security rule, be subject to the Federal Energy Regulatory Commission (FERC) approved North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) reliability standards. As discussed in the COM, "there is a common objective and associated advantages of having the NRC as the single Federal entity regulating and inspecting cyber security onsite at NRC-licensed NPPs."

We recognize that this policy change expanded the scope of assets included in the cyber security program beyond those strictly necessary to prevent radiological sabotage. However, on this matter industry continues to support having the NRC as the single regulatory authority for cyber security at NRC-licensed nuclear power plants. The change proposed in this Petition is not intended to, and does not undermine the regulatory efficiency discussed in the COM.

[5] COMWCO-10-001, "Regulation of Cyber Security at Nuclear Power Plants," from Commissioner Ostendorff to then-Chairman Jaczko and the other NRC Commissioners, was intended to "facilitate a policy decision by the Commission related to the NRC's, the Federal Energy Regulatory Commission's (FERC), and the North American Electric Reliability Corporation's (NERC) responsibilities for cyber security regulation, enforcement, and inspection." Commissioner Ostendorff recommended that the Commission make a policy decision to expand the scope of the cyber security rule in Section 73.54 such that SSCs located in the Balance-of-Plant at NRC power reactors should be included within the scope of that rule.

E. Granting this Petition Will Enhance Regulatory Clarity

NRC licensees are implementing their cyber security plans using a uniform schedule divided into eight milestones. The first seven milestones were implemented by each nuclear power plant on or before December 31, 2012. Collectively, these seven milestones put into place the key protective measures of the cyber security program, with a particular emphasis on detailed assessments and implementation of protective measures for digital assets that could adversely impact equipment in target sets. The eighth milestone, "Milestone 8," which is ongoing, implements the balance of the program. It includes detailed assessments of the remaining (in some cases, thousands) digital assets, and includes the establishment of the elements necessary to maintain the implemented cyber security program.

In January 2013 the NRC began inspecting licensees' implementation of the seven milestones. By March 1, 2014, the NRC had conducted 24 inspections at nuclear power plants located in each of the four NRC regions. As a result of these inspections, the NRC staff has identified a number of violations of low safety significance associated with licensees' failure to identify digital assets that the NRC believes must be protected against cyber attacks based on the current rule language. The NRC identified 20 violations at 17 sites associated with Milestone 2 – the principal milestone for identifying digital assets requiring protection. The NRC has also identified 21 violations at 18 sites associated with Milestone 6, which includes the identification and protection of digital assets that could impact target sets. Of the 21 violations, 13 are directly associated with digital asset identification. The combined 33 Milestone 2 and Milestone 6 violations illustrate the problem created by the language in 10 CFR 73.54(a)(1), despite the availability of endorsed guidance. Although these violations have little to no safety significance, they have caused unnecessary expense, diverted licensee resources, and have conveyed to the public an incorrect impression that the state of cyber security preparedness at those sites is less than adequate.

F. Analysis of Existing Section 73.54 and Proposed Changes to Section 73.54

The following provides a comparison between the current rule text in 10 CFR 73.54 (a) and NEI's suggested revision of that language.

Section 73.54(a) Current Rule: Each licensee subject to the requirements of this section shall provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in § 73.1.
(a) Proposed Rule: No change

Effect of Proposed Revision to 73.54(a):
The current language contains the appropriate link between the cyber security program and the need to protect against the design basis threat of radiological sabotage cyber attack. Accordingly, no changes are necessary.

Section 73.54(a)(1) Current Rule: The licensee shall protect digital computer and communication systems and networks associated with:
(a)(1) Proposed Rule: The licensee shall protect digital computer and communication systems and networks associated with structures, systems, or components:

Effect of Proposed Revision to 73.54(a)(1):
The proposed change would insert "structures, systems, or components." 10 CFR 73.54 provides the programmatic requirements to defend against the design basis threat of radiological sabotage cyber attack. As an integrated component of the physical protection program, the cyber security program is designed to prevent significant core damage and spent fuel sabotage. To prevent significant core damage and spent fuel sabotage, licensees may rely on plant structures, systems, or components to perform certain functions. Through the analysis required by 10 CFR 73.54(b)(1), the cyber security rule must be implemented to identify those digital computer and communication systems and networks that, if subject to the cyber attack described in 10 CFR 73.54(a)(2), would adversely impact the capability for systems and equipment to perform their intended function to prevent significant core damage and spent fuel sabotage. Licensees must include and protect those identified digital computer and communications systems and networks in the cyber security program implemented to meet the requirements of this Section.

Section 73.54(a)(1)(i) Current Rule: Safety-related and important-to-safety functions.
(a)(1)(i) Proposed Rule: That are necessary to prevent significant core damage and spent fuel sabotage.

Effect of Proposed Revision to 73.54(a)(1)(i): The requirement is revised to more clearly define the set of equipment that must be protected against the effects of the design basis threat of radiological sabotage cyber attack. This change would align the set of systems and equipment protected against the effects of a cyber attack with the set of systems and equipment protected against effects of the other attributes of the design basis threat of radiological sabotage described in 10 CFR 73.1.

Section 73.54(a)(1)(ii) Current Rule: Security functions.
(a)(1)(ii) Proposed Rule: Whose failure would cause a reactor scram.

Effect of Proposed Revision to 73.54(a)(1)(ii): The current rule requirement is deleted and replaced by the proposed change to 10 CFR 73.54(a)(1)(i), which requires licensees to protect digital computer and communication systems and networks associated with the systems and equipment necessary to prevent significant core damage and spent fuel sabotage. The proposed change would be added to require licensees to continue to include within the cyber security program certain balance-of-plant structures systems and components considered in COMWCO-10-001, dated September 14, 2010, even though this equipment may not be necessary to prevent radiological sabotage. The assets that should be considered would be those whose failure to perform their intended function would result in a reactor trip. The proposed requirement would identify the set of plant structures, systems, or components out to the first intertie with the offsite transmission system that, if not included within the cyber security program, would be subject to the Federal Energy Regulatory Commission-approved Critical Infrastructure Protection Reliability Standards.

Section 73.54(a)(1)(iii) Current Rule: Emergency preparedness functions, including offsite communications.
(a)(1)(iii) Proposed Rule: None

Effect of Proposed Revision to Section 73.54 (a)(1)(iii): The current rule requirement is deleted and replaced by the proposed change to 10 CFR 73.54(a)(1)(i), which requires licensees to protect digital computer and communication systems and networks associated

with the systems and equipment necessary to prevent significant core damage and spent fuel sabotage.

Section 73.54(a)(1)(iv) Current Rule: Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.
(a)(1)(iv) Proposed Rule: None.

Effect of proposed Revision to Section 73.54(a)(1)(iv): The current rule requirement is deleted and replaced by the proposed change to 10 CFR 73.54(a)(1)(i), which requires licensees to protect digital computer and communication systems and networks associated with the systems and equipment necessary to prevent significant core damage and spent fuel sabotage.

Proposed Language Amending 10 CFR 73(a):

We request that the NRC amend section 10 CFR 73.54(a) as follows:

(*a) Each licensee subject to the requirements of this section shall provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in § 73.1.*

(1)The licensee shall protect digital computer and communication systems and networks associated with structures, systems, or components:

(i) That are necessary to prevent significant core damage and spent fuel sabotage; or

(ii) Whose failure would cause a reactor scram.

~~(i) Safety-related and important-to-safety functions;~~

~~(ii) Security functions;~~

~~(iii) Emergency preparedness functions, including offsite communications; and~~

~~(iv) Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions."~~