November 15, 2012

Mr. David R. Kline
Director, Security
Nuclear Energy Institute
1776 I Street, NW
Suite 400
Washington, DC 20006

SUBJECT: NUCLEAR ENERGY INSTITUTE RESPONSE TO THE U.S. NUCLEAR REGULATORY COMMISSION'S JULY 27, 2012, LETTER REGARDING NEI 10-04, "IDENTIFYING SYSTEMS AND ASSETS SUBJECT TO THE CYBER SECURITY RULE," REVISION 2

Dear Mr. Kline:

In a letter dated August 22, 2012, the Nuclear Energy Institute (NEI) requested that the U.S. Nuclear Regulatory Commission (NRC) withdraw the two exceptions stated in its July 27, 2012, letter regarding NEI 10-04, "Identifying Systems and Assets Subject to the Cyber Security Rule," Revision 2. The basis for this request is NEI's assertions that the digital systems and equipment implementing the security programs identified in Title 10 of the *Code of Federal Regulations* (10 CFR) 73.55(b) and certain non-permanently installed devices, including digital Maintenance and Test Equipment (M&TE), are not within the scope of the NRC's cyber security rule. NEI asserts that including these systems and equipment within the scope of the rule would require the protection of assets that have no nexus to radiological or spent fuel sabotage and is therefore inconsistent with the agency's past interpretation of the scope of the cyber security rule. The NRC does not agree with these assertions. The basis of our disagreement is provided below.

The NRC agrees with NEI that the central focus of the cyber security rule is the prevention of radiological sabotage. Consistent with this focus, 10 CFR 73.54(a) requires that licensees 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. The NRC also agrees with NEI that the cyber security rule does not prescribe a specific list of digital systems and equipment subject to the requirements of 10 CFR 73.54. However, NEI looks to some explanatory language in the 2006 proposed rule for Power Reactor Security Requirements to support its assertion that the scope of the NRC's cyber security rule is limited to protecting computers performing security functions of a plant's onsite physical protection system. The NRC does not agree that the explanatory language quoted by NEI in its August 22, 2012, letter was intended by the Commission to limit the scope of the rule to computers associated with a plant's onsite physical protection system. Furthermore, such an interpretation is inconsistent with the current language of 10 CFR 73.54(a)(1).

The language of the final cyber security rule published in the *Federal Register* on March 27, 2009, included many changes to the rule language originally proposed in 2006. These changes included language in 10 CFR 73.54(a)(1) requiring that licensees protect from cyber attack those digital computer and communication systems and networks associated with safety, security and emergency preparedness (SSEP) functions and support systems and equipment which, if compromised, would adversely impact SSEP functions. Such support systems are broader than a plant's onsite physical protection system, and potentially include the digital systems and equipment identified in 10 CFR 73.55(b).

In accordance with 73.54(b)(1) and Section C.3.1.3 "Identification of Critical Digital Assets" of Regulatory Guide (RG) 5.71, a licensee must perform analyses to determine whether compromise of a plant's digital systems and equipment could adversely impact SSEP functions, or serve as a pathway to a critical system (CS) or critical digital asset (CDA) performing a SSEP function. A licensee can only determine that a particular digital system or equipment is not a CS or CDA once this analysis is performed and demonstrates that the compromise, exploitation, or failure of the system or equipment would not adversely impact SSEP functions. This includes analysis of the plant's onsite physical protection systems and those digital systems and equipment associated with the licensees' physical protection program. For this reason, the NRC does not agree that the digital systems and equipment identified in 10 CFR 73.55(b) can be categorically excluded from the scope of the cyber security rule. Furthermore, consistent with 10 CFR 73.54(b), it is the licensee's responsibility to implement this analysis.

In your August 22, 2012, letter you stated that the NRC's position on the digital systems and equipment identified in 10 CFR 73.55(b) raises backfit implications because it implies that licensees would have to protect digital systems and equipment that have no nexus to radiological sabotage. This is a misinterpretation of the basis of the NRC's exception to Section 2.2 of NEI 10-04, Revision 2. As discussed above, the NRC agrees that the digital systems and equipment identified in 10 CFR 73.55(b) would not have to be protected in accordance with the requirements in 10 CFR 73.54 if a licensee's analysis demonstrates that the compromise, exploitation, or failure of these systems or equipment would not adversely impact an SSEP function. Since the final publication of 10 CFR 73.54, the NRC's position on cyber security and the protection of security functions and support systems from cyber attacks has not changed, nor does the NRC require that industry meet requirements outside of the current NRC regulations. Therefore, the NRC does not agree that the basis for its exception to Section 2.2 "Security Systems" in NEI 10-04, Revision 2 constitutes a backfit as defined under 10 CFR 50.109, "Backfitting."

With respect to the NRC's second exception to NEI 10-04, your August 22, 2012, letter stated that "NEI 10-04 presumes that support systems and equipment are permanently installed plant equipment." Based on this presumption, NEI concluded that "non-permanently installed devices (including Maintenance and Test Equipment M&TE) would not be identified as critical systems (CS) or Critical Digital Assets (CDAs)." NEI revised the July 2012 version of NEI 10-04 to reflect this presumption. However, there is no language in 10 CFR 73.54, or in any cyber security guidance published by the agency or endorsed by the NRC as acceptable for use by licensees, to support NEI's presumption that non-permanently installed digital devices, including M&TE, are outside the scope of the NRC's cyber security rule. Furthermore, NEI's August 22, 2012, letter specifically recognized the cyber security risks associated with these types of devices.

Section C.3.1.3 of RG 5.71 identifies as a CDA those digital assets that: (1) could adversely affect SSEP functions, or (2) could provide a pathway to a CS or a CDA that could be used to compromise, attack, or degrade an SSEP function. Section C.3.1.3 further notes that a CDA may be directly or indirectly connected to a CS. Consistent with this language, any digital asset that has a direct or indirect connection to a CDA can serve as a pathway for compromising that CDA through a cyber-based attack. This includes digital assets that connect, even temporarily, to a CS or CDA and can introduce risks equivalent to those posed by permanently connected systems and equipment.

The NRC recognizes that not all non-permanently installed digital assets are CDAs. Consistent with 10 CFR 73.54(b), a licensee must conduct a site specific analysis of digital computer systems and networks to identify assets that must be protected in accordance with 10 CFR 73.54(a)(1). If, on the basis of this analysis, the licensee determines that a non-permanently installed digital device has the potential to adversely impact the integrity or function of a SSEP system, or can serve as a pathway to compromise, attack or degrade an SSEP function, it must protect that digital device in accordance with the requirements set forth in 10 CFR 73.54.

At this time, the NRC considers its review of NEI 10-04, Revision 2 closed. The information provided in NEI's August 22, 2012, letter does not set forth an adequate basis for withdrawing the two exceptions specified in the NRC's July 27, 2012, letter to NEI. As stated in the NRC letter dated July 27, 2012, the NRC intends to endorse NEI 10-04 in a future revision that appropriately gives due consideration to the exceptions cited in that letter for RG 5.71 Sections 2.2, "Security Systems," and Section 2.4 "Support Systems and Equipment."

We look forward to working with you in achieving a successful implementation of cyber security programs at licensee facilities. Should you or your staff have any questions, please contact Craig Erlanger at (301) 415-5374 or Eric Lee at (301) 415-8099.

Sincerely,

/RA/

Christiana Lui, Director
Division of Security Policy
Office of Nuclear Security
and Incident Response

Section C.3.1.3 of RG 5.71 identifies as a CDA those digital assets that: (1) could adversely affect SSEP functions, or (2) could provide a pathway to a CS or a CDA that could be used to compromise, attack, or degrade an SSEP function. Section C.3.1.3 further notes that a CDA may be directly or indirectly connected to a CS. Consistent with this language, any digital asset that has a direct or indirect connection to a CDA can serve as a pathway for compromising that CDA through a cyber-based attack. This includes digital assets that connect, even temporarily, to a CS or CDA and can introduce risks equivalent to those posed by permanently connected systems and equipment.

The NRC recognizes that not all non-permanently installed digital assets are CDAs. Consistent with 10 CFR 73.54(b), a licensee must conduct a site specific analysis of digital computer systems and networks to identify assets that must be protected in accordance with 10 CFR 73.54(a)(1). If, on the basis of this analysis, the licensee determines that a non-permanently installed digital device has the potential to adversely impact the integrity or function of a SSEP system, or can serve as a pathway to compromise, attack or degrade an SSEP function, it must protect that digital device in accordance with the requirements set forth in 10 CFR 73.54.

At this time, the NRC considers its review of NEI 10-04, Revision 2 closed. The information provided in NEI's August 22, 2012, letter does not set forth an adequate basis for withdrawing the two exceptions specified in the NRC's July 27, 2012, letter to NEI. As stated in the NRC letter dated July 27, 2012, the NRC intends to endorse NEI 10-04 in a future revision that appropriately gives due consideration to the exceptions cited in that letter for RG 5.71 Sections 2.2, "Security Systems," and Section 2.4 "Support Systems and Equipment."

We look forward to working with you in achieving a successful implementation of cyber security programs at licensee facilities. Should you or your staff have any questions, please contact Craig Erlanger at (301) 415-5374 or Eric Lee at (301) 415-8099.

Sincerely,

/RA/

Christiana Lui, Director
Division of Security Policy
Office of Nuclear Security
and Incident Response

DISTRIBUTION:
DSP r/f

ADAMS Accession Number: ML12257A454

OFFICE	NSIR/DSP	NSIR/DSP	NSIR/DSP
NAME	ELee	CErlanger	RFelts
DATE	9/19/12 11/13/12	9/19/12	9/19/12 11/13/12
OFFICE	NSIR\DSO	OCG	NSIR/DSP
NAME	PHolahan	NStAmour	CLui
DATE	9/21/12 11/13/12	11/13/12	11 /15/12

OFFICIAL RECORD COPY