July 27, 2012

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

SUBJECT: NUCLEAR ENERGY INSTITUTE 10-04, "IDENTIFYING SYSTEMS AND ASSETS SUBJECT TO THE CYBER SECURITY RULE," REVISION 2

Dear Mr. Kline:

In your letter dated June 27, 2012, you requested that the U.S. Nuclear Regulatory Commission (NRC) staff review and endorse the Nuclear Energy Institute's (NEI's) guidance document NEI 10-04, "Identifying Systems and Assets Subject to the Cyber Security Rule," Revision 2, dated July 2012 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML12180A081). This July 2012 version of NEI 10-04, Revision 2 was submitted in response to NRC staff comments provided to NEI by a letter dated May 31, 2012 (ADAMS Accession No. ML12145A607).

The NRC staff completed the review of the NEI 10-04, Revision 2 using NRC security regulations, regulatory guidance, and industry guidance determined by the NRC to be acceptable for use by industry in meeting the requirements of Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54. A list of these documents is provided as Enclosure 1. Based on the review, the staff concluded that the NEI 10-04, Revision 2 did not adequately address four of the staff's comments provided on May 31, 2012, specifically comments 8, 9, 10, and 18. These comments from the NRC's May 31, 2012, letter to NEI are provided in Enclosure 2.

The NRC staff concludes that the NEI 10-04, Revision 2 is acceptable for use by licensees to identify critical digital systems and critical digital assets with the following two exceptions:

1. Section 2.2 "Security Systems"

The NEI 10-04, Revision 2 does not include all of the security systems that are within the scope of 10 CFR 73.54. Specifically, certain digital systems and equipment associated with security functions defined under 10 CFR 73.55(b) are explicitly excluded in the document. The NEI 10-04, Revision 2 states that digital computing systems used to facilitate the establishment, maintenance, and implementation of the following programs required under 10 CFR 73.55(b) are not within the scope of the Cyber Security Rule:

- Performance Evaluation Program
- Access Authorization Program
- Insider Mitigation Program
- Corrective Action Program

The NEI 10-04 Revision 2 incorrectly excludes these digital computing systems by stating the following:

> *Licensees may use digital computing systems to facilitate the implementation of these other requirements in 10 CFR 73.55. These systems, however, are not a part of the onsite physical protection system, are not associated with the capability to detect, assess, interdict, and neutralize threats up to and including the design basis threat of radiological sabotage as stated in 10 CFR 73.1, and the failure or compromise of these information systems cannot lead to a radiological sabotage event.*

The digital systems and equipment used to facilitate the implementation of security programs specified in 10 CFR 73.55(b) are within the scope of 10 CFR 73.54. However, 10 CFR 73.54(b) allows licensees to protect only those systems that, if compromised, could lead to adverse impact to the safety-related, important-to-safety, security, or emergency preparedness functions as specified in 10 CFR 73.54 (a). Once the licensees determine that a particular digital asset must be protected, the NRC approved licensees' cyber security plans and Section C.3.3 of Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities," provide licensees flexibility in addressing potential cyber security threats and vulnerabilities.

The flexibility in addressing the security controls includes taking credit for existing programs that incorporate applicable security controls or deploying other alternative measures, as long as the alternative measures provide equal or greater protection as the corresponding control in the NRC approved cyber security plans. I encourage licensees to use the NRC Security Frequently Asked Question program for further clarification on site specific conditions and issues associated with implementing their cyber security programs.

2. Section 2.4 "Support Systems and Equipment"

As part of the comments in Enclosure 2, the staff provided a clarification to NEI 10-04, Revision 2 that digital systems and equipment that provide a pathway to critical systems are within the scope of the 10 CFR 73.54, in accordance with the definition of a critical digital asset in Appendix B of NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6. This includes digital test and maintenance equipment for safety and safety-related systems whose connections to critical systems may not be permanent, but the compromise of which could have an adverse impact on digital systems performing safety functions at the plant. This comment was not addressed or incorporated in the July 2012 version of NEI 10-04, Revision 2. This clarification is necessary to avoid potential future misinterpretations during the NRC oversight activities.

The July 2012 NEI 10-04, Revision 2, along with the above two described exceptions, provide acceptable guidance for licensees to use for identifying those critical digital systems and critical digital assets require protection under the NRC Cyber Security Rule. The NRC requests that NEI transmit these two exceptions along with the July 2012 version of NEI 10-04, Revision 2 to all operating power reactor licensees and combined license applicants. Formal endorsement of the NEI 10-04, Revision 2 is planned in a future update to RG 5.71.

Please contact Craig Erlanger at (301) 415-5374 or Eric Lee at (301) 415-8099 if you have any questions.

Sincerely,

/RA/

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

Enclosures:
1. Documents Supporting the Review
2. NRC Staff Comments on the April 2012 Version of NEI 10-04 Revision 2

Please contact Craig Erlanger at (301) 415-5374 or Eric Lee at (301) 415-8099 if you have any questions.

Sincerely,

/RA/

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

Enclosure:
1. Documents Supporting the Review
2. NRC Staff Comments on NEI 10-04 Revision 2

ADAMS Accession No.: ML12198A198 (Pkg) ML12194A532 (Memo) ML12198A192 (Enl 2)

OFFICE	NSIR/DSP	NSIR/DSP	NSIR/DPR	NSIR/DSO
NAME	ELee	D. Parsons for/CErlanger	RLewis	PHolahan
DATE	7/16/12	7/16/12	7/19/12	7/12/12
OFFICE	NRO/DE	NRR/DE	OGC	NSIR/DSP
NAME	TBergman	PHiland	NStAmour	CLui
DATE	7/16/12	7/20/12	7/27/12	7/27/12

OFFICIAL RECORD COPY

Documents Supporting the Review

Title 10 Code of Federal Regulations Part 73.54, “Protection of Digital Computer and Communication Systems and Networks,” U.S. Nuclear Regulatory Commission, Washington, DC.

Title 10 Code of Federal Regulation Part 73.55, “Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage,” U.S. Nuclear Regulatory Commission, Washington, DC.

Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Facilities,” U.S. Nuclear Regulatory Commission. January 2010.

NEI 08-09, “Cyber Security Plan for Nuclear Power Reactors,” Revision 6, Nuclear Energy Institute. April 2010

NEI 03-01, “Nuclear Power Plant Access Authorization Program,” Revision 3, Nuclear Energy Institute. May 2009