WILLIAM R. GROSS
Director, Incident Preparedness

1201 F Street, NW, Suite 1100
Washington, DC 20004
P: 202.739.8123
wrg@nei.org
nei.org

NUCLEAR ENERGY INSTITUTE

SUNSI Review Complete
Template = ADM-013
E-RIDS=ADM-03
ADD= Jazel Parks, Bayssie Mekonen

COMMENT (12)
PUBLICATION DATE: 8/23/2018
CITATION # 83 FR 42623

October 19, 2018

Ms. May Ma
Office of Administration
Mail Stop: ON 2A13
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Comments on Draft Regulatory Guide 5061, "Proposed Revision 1 to Regulatory Guide 5.71, Cyber Security Programs for Nuclear Power Reactors" (NRC Docket ID NRC-2018-0182)

Project Number: 689

Dear Ms. Ma:

On behalf of the Nuclear Energy Institute's (NEI)[1] members (hereinafter referred to as industry), we provide the following comments on Draft Regulatory Guide (DG)-5061, "Proposed Revision 1 to Regulatory Guide 5.71, Cyber Security Programs for Nuclear Power Reactors," as requested in the Federal Register (83FR42623), dated August 23, 2018.

On or before December 31, 2012, the U.S. Nuclear Regulatory Commission (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. Subsequently, on or before December 31, 2017, NRC power reactor licensees completed the remainder of the cyber security program.

Industry experience from the inspections conducted by the NRC following the December 31, 2012, milestone indicated that gaps existed between the NRC's and the industry's interpretation of compliance with the cyber security rule. While progress has been made, the inspections following the December 31, 2017, milestone have demonstrated that this gap continues to exist. NEI believes that the purpose of any revision to Regulatory Guide (RG) 5.71 should bridge that gap. However, a wholesale rewrite of the regulatory guide is simply not needed at this time.

[1] The Nuclear Energy Institute (NEI) is responsible for establishing unified policy on behalf of its members relating to 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, major architect and engineering firms, fuel cycle facilities, nuclear materials licensees, and other organizations involved in the nuclear energy industry.

NEI recognizes the NRC's desire to provide improved guidance for future licensees and appreciates its willingness to invest in that effort, however, in view of the limited number of currently expected new licensees in the near-term, we believe that both the NRC's and the industry's resources would be better utilized by continuing to concentrate on resolving issues related to the existing reactor fleet rather than revising the existing guidance.

While we understand the staff's intent, that the revised guidance will not present any change to the current reactor fleet, the fact that the revised guidance exists may create the potential for some inspectors to believe it supersedes the existing guidance such that the inspectors apply it—rather than the existing guidance—during inspections.

In addition, if new applicants who are part of an existing nuclear utility are scrutinized against this new guidance, existing sites within that fleet may also be expected to comply with the new guidance.

The NEI Cyber Security Task Force has conducted a preliminary review of the draft guide and has identified a number of concerns. Notably, this new guidance does not consider the recommendation from the NRC Advisory Committee on Reactor Safeguards (ACRS) for use of Probabilistic Risk Assessment (PRA) insights in cyber security, particularly those regarding accident sequences.[2]

The task force identified changes in staff position. Specifically, the new guidance indicates that certain digital devices that are not currently identified as Critical Digital Assets (CDAs) may need to be considered CDAs for future licensees.

Security definitions in the glossary differ from previously NRC issued definitions contained in NUREG-2203, "Glossary of Security Terms for Nuclear Power Reactors." The definitions should be consistent within NRC issued documents.

Additionally, Appendix A, Section A.3.1.6, continues to require application of all of the security controls, allows the use of alternative controls only if the security control could not be applied, and requires that the alternative control countermeasures provide the same or greater protection as the corresponding security control. This section establishes additional requirements over and above the regulation for maintaining the security plan,[3] is not consistent with the existing NRC endorsed guidance[4] for evaluating the use of alternative countermeasures, and does not incorporate risk-based screening of CDAs and application of cyber security protections.[5]

NEI understands that the NRC intends to conduct a thorough and aggressive self-assessment of the cyber security inspection process, including the efficacy of the guidance, starting in January 2019. In view of this

[2] The U.S. NRC Advisory Committee on Reactor Safeguards letter to G. B. Jaczko, Chairman U.S. NRC, "Draft Final Regulatory Guide 5.71, 'Cyber Security Programs for Nuclear Facilities,'" dated November 12, 2009 (ADAMS Accession No. ML093130111)
[3] 10 CFR 50.54(p)
[4] Reference NEI 08-09, Revision 6, Addendum 1
[5] Reference NEI 13-10, Revision 6

upcoming work scope, which undoubtedly will result in additional desired changes to RG 5.71, NEI urges the NRC to wait until after the self-assessment to revise the regulatory guide. Additionally, the revision should address risk-informing the cyber security plans and should formally endorse the existing NEI guidance documents.

Regulatory activities should be consistent with the degree of risk reduction and regulatory certainty that they achieve, and in that regard, this document revision has no clarifying or beneficial impact on the current reactor fleet. It does, however, have the potential to create an unintended consequence of confusion regarding what changes should apply to the current reactor fleet.

Given the other cyber security issues in which the NRC and NEI are currently productively engaged, the revision of the regulatory guide should not be pursued until after the NRC completes the self-assessment in 2019. Reviewing, commenting on and revising the regulatory guide at this time may detract from the other higher priority resolution of issues identified during the cyber security inspections. NEI suggests that the resolution of these issues, and the results of the 2019 self-assessment, also be included in the revision to the regulatory guide.

If you have any questions concerning these comments, please contact Richard Mogavero at (202) 739-8174 or rm@nei.org, or me.

Sincerely,

William R. Gross