PUBLIC SUBMISSION

SUNI Review Complete
Template=ADM-013
E-RIDS=ADM-03

ADD: Bridget Curran, Mekonen Bayssie, Mary Neely
Comment (2)
Publication Date: 3/3/2022
Citation: 87 FR 12208

As of: 5/4/22 9:36 AM
Received: May 02, 2022
Status: Pending_Post
Tracking No. l2o-wrae-po2c
Comments Due: May 02, 2022
Submission Type: Web

Docket: NRC-2021-0143
Cyber Security Programs for Nuclear Power Reactors

Comment On: NRC-2021-0143-0001
Cyber Security Programs for Nuclear Power Reactors

Document: NRC-2021-0143-DRAFT-0004
Comment on FR Doc # 2022-04464

Submitter Information

Email: kme@nei.org
Organization: Nuclear Energy Institute

General Comment

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-2021-0143).

Attachments

05-02-22_Comments on DG-5061.R1

RICHARD MOGAVERO
Senior Project Manager, Nuclear Security & Incident Preparedness

1201 F Street, NW, Suite 1100
Washington, DC 20004
P: 202.739.8174
rm@nei.org
nei.org

NUCLEAR ENERGY INSTITUTE

May 2, 2022

Office of Administration
Mail Stop: TWFN–7– A60M
U.S. Nuclear Regulatory Commission Washington, DC 20555-0001
ATTN: Program Management, Announcements and Editing Staff

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-2021-0143)

Project Number: 689

Submitted via Regulations.gov

Program Management, Announcements and Editing Staff

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 (87FR12208), dated March 3, 2022.

On or before December 31, 2017, the U.S. Nuclear Regulatory Commission (NRC) power reactor licensees completed implementation of the cyber security program. Industry experience from the inspections conducted by the NRC following the December 31, 2017, milestone indicated that gaps existed between the NRC's and the industry's interpretation of compliance with the cyber security rule. To address the gaps, the NEI Cyber Security Task Force developed, and the NRC staff reviewed and found acceptable for use, four

[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.

white papers related to Emergency Preparedness[2], Balance of Plant[3], Safety-Related/Important-to-Safety[4], and Security[5] digital assets. The associated white paper changes were then captured in updates to NEI guidance documents NEI 10-04, Revision 3 and NEI 13-10, Revision 7. These revisions were then submitted to the NRC on behalf of the industry and are currently under NRC review. NEI believes the NRC should delay issuance of this regulatory guide until the NRC completes their review and approval of the aforementioned NEI documents.

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 NRC approved licensee cyber security program—during inspections. Actions should be taken to prevent this confusion during inspections.

NEI comments are contained in the Attachment. In particular, the document does not acknowledge NEI 08-09 or capture the agreed upon changes in the associated Addenda as acceptable for use by the NRC. Further, with consideration given to the graded approach to cyber security that the Federal Energy Regulatory Commission has incorporated regarding power generators and the subsequent changes made in the Balance of Plant NEI white paper, these risk-informed changes should be addressed in the section of the regulatory guide focused on the "Balance of Plant."

This revised guidance adds "Control Intent" wording to each of the Appendix B technical and Appendix C operational and management cyber security controls. The industry remains concerned that this added wording will now create inspection concerns and unnecessary discussions between the "Control Intent" and the licensees cyber security program documents and procedures.

As the industry seeks to innovate using new and technology for improved safety and efficiency of operations, the NRC should consider removing the prohibition for wireless communication associated with Safety-Related and Important-to-Safety systems and allow its use with appropriate cyber security controls.

Lastly, regulatory activities should be consistent with the degree of risk reduction and regulatory certainty that they achieve, and in that regard, this document has the potential to create an unintended consequence of confusion regarding what changes should apply to the current reactor fleet.

---

[2] ADAMS Accession No. ML20129J981
[3] ADAMS Accession No. ML20209A442
[4] ADAMS Accession No. ML20223A256
[5] ADAMS Accession No. ML21140A140

If you have any questions concerning these comments, please contact me.

Sincerely,

Richard Mogavero

Attachment

c: Duane Wright, NRC/NSIR
Kim Lawson-Jenkins NRC/NSIR

#	Page	Section	Proposed Change/ New Language	Comment/ Justification
1		General		Based on the significant changes proposed in NEI 10-04, Revision 3 and NEI 13-10, Revision 7, the NRC should consider delaying issuance of RG 5.71 until the NRC completes the review and approval of both NEI documents.
2		General		The document uses "safety" and "safety-related" interchangeably throughout document; the industry recommends revising RG 5.71 for consistency with the NRC-approved NEI White Paper focused on the identification and protection of digital assets associated with Safety-Related (SR) and Important-to-Safety (ITS) functions.
3	1	Applicability		There is a comma at the end of the sentence causing confusion to the reader. Did the NRC intend on providing additional information? Or should this be a period?
4	7			RG 5.71, Revision 1 should note that NEI 08-09 and the associated Addendums have been found to be acceptable for use by the NRC.
6	7			Although noted later in document, the Background Section should state that NEI 13-10 has been found to be acceptable for use by the NRC.
7		General		NEI 08-09, Addendum 1 contained changes based on nuclear plants being in a "production environment," these changes do not appear to be captured in this revision of RG 5.71.
8	14	C.3	To the second bullet in the final set of bullets in Section C.3 just prior to Section C.3.1, add "… as specified in RG 5.60"	Bullet should read "characterization of threats to the facility as specified in RG 5.69" with applicable reference to the guide.
9	19			This revision of RG 5.71 does not address that the Federal Energy Regulatory Commission's (FERC) has incorporated a graded approach to cyber security and has revised needed cyber security controls for generators accordingly. This should be addressed within the Balance of Plant (BOP)

				sections within the document. This would also include discussing the 15-minute shutdown guidance in the NRC approved NEI White Paper focused on the identification and protection of digital assets associated with Balance of Plant functions.
10	19		Should be "and"	Page 19 and Figures 4 and 5, as well as other parts of the document, state BOP criteria as "and" and "or." This should be consistent throughout document
11	18			Figure 3, BOP and ITS should not be under safety systems, this should be at a higher level.
12	21	Figure 5	Remove bubble "Affects Critical Assets, Functions and/or Pathways."	There is no guidance in DG-5061 that discusses how this decision block should be interpreted. It appears to be redundant with the "Performs…" and "Supports…" decision blocks.
13	40			Section C.4.1.2 added a discussion on metrics; the NRC should consider clarifying that metrics are not required to address the control and are optional.
14	Appendices B and C	Appendices B and C	Remove Appendix B and Appendix C	NEI recommends the NRC eliminate Appendices B and C. Licensees should be free to use security control sets by NIST, NERC, IAES, ISO, IEE, IEC, or other credible external organizations. This will reduce prescriptiveness and increase efficiency in overall implementation.
15	B-9			The NRC should consider removing the prohibition for wireless communication associated with Safety-Related and Important-to-Safety systems and allow its use with appropriate cyber security controls.
16		General		The term "Intent of Control" – was added to all controls. Where was this definition derived? The industry is concerned that this added wording will now create inspection concerns and unnecessary discussions between the "Control Intent" and the licensees cyber security program documents and procedures.
17	Glossary			Many definitions were added to this document, examples being: • Attack Pathway • Attack Surface • Attack Vector • Portable Media Where did the definitions come from?

18	Glossary			The definition of cyber attack changed; there are now three definitions, Rev 0, Rev 1, and NEI 08-09. The industry recommends using one consistent definition, that being the NEI 08-09 definition.
19	Glossary			The definition of support system should note the change in the NRC approved NEI White Paper focused on the identification and protection of digital assets associated with Safety-Related (SR) and Important-to-Safety (ITS) functions.
20	5	B		A revision log should be added to RG 5.71, Revision 1 identifying the significant changes, additions, and deletions made to Revision 0 of RG 5.71. The section "Reason for Revision" provides a very high level summary of the RG update, but does not identify the specific revisions. NIST SP800-53, Rev 4 provides a good example of such a log listing significant revisions.