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

March 1, 2023

Mr. Brian M. Yip
Chief, Cyber Security Branch,
Division of Physical and Cyber Security Policy
Nuclear Security and Incident Response
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Wireless Cyber Security Guidance
Reference: NEI 08-09

Project Number: 689

Dear Mr. Yip:

On behalf of our members, the Nuclear Energy Institute (NEI)[1] is examining the cybersecurity protections for wireless devices used for the monitoring, but not control, of equipment in operating nuclear plants.

The NRC's cyber security regulation, 10 CFR 73.54, is silent on wireless communications. However, an NEI guidance document, NEI 08-09, Revision 6, includes a cyber security control that prohibits using wireless communications for certain applications[2]. At the same time, NEI 08-09, Section 3.1, allows for implementing "alternative controls" and countermeasures that eliminate the applicable cyber threat/attack vectors.

NEI believes that licensees should address the following cybersecurity controls to eliminate the threat/attack vectors relevant to deployment of wireless communication technology associated with monitoring. The licensees should, in accordance with their cyber security plan, implement the appropriate technical cyber security controls, document that the wireless approach maintains the current defensive architecture, and address the unique aspects of their Radio Frequency (RF) spectrum controls relevant to the wireless devices employed.

[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.
[2] The prohibition is stated in Section D.1.17 of NEI 08-09, Rev. 6, "Cyber Security Plan for Nuclear Power Reactors", April 2010. NEI 08-09, Rev. 6, is available in the NRC ADAMS system under accession number ML101180437.

The following table includes technical controls for securing both wired and wireless communications technology associated with monitoring. The first 10 controls listed are already described in NEI 08-09. The three additional controls listed after them are recommended by cyber security subject matter experts at the U.S. Department of Energy (DOE)[3].

Technical Cyber Security Controls in NEI 08-09	Wired Network	Wireless Network
D.2.8 Time stamps	√	√
D.3.2 Application partitioning/security function isolation	√	√
D.3.3 Shared resources	√	√
D.3.4 Denial-of-service protection	√	√
D.3.5 Resource priority	√	√
D. 3.6 Transmission integrity	√	√
D.3.7 Transmission confidentiality	√	√
D.3.8 Trusted path	√	√
D.3.9 Cryptographic key establishment and management	√	√
D.3.17 Session authenticity	√	√
Proposed Additional Controls for Wireless Monitoring Devices		
Radio Resource management		√
RF monitoring		√
RF-restricted zones		√

NEI asks that the NRC find this approach of implementing the above cybersecurity controls from NEI 08-09, Revision 6, and the additional three controls that address the RF spectrum, acceptable to eliminate the threat/attack vectors associated with the D.1.17 control. This will give users confidence that potential wireless monitoring devices can be considered.

At this time NEI does not intend for users to replace installed wired technologies nor bypass the existing cybersecurity defensive architecture of safety-related and important-to-safety critical digital assets. There is no intent for wireless devices to bypass any one-way deterministic device or airgaps that segregate safety-related or important-to-safety critical digital assets.

NEI respectfully requests that NRC respond to this letter in writing. Because this effort is integral to the project to revise NEI 08-09[4], we request that this review be performed under the approved fee exemption for NEI 08-09, Revision 7[5].

The NRC's reply would be most helpful to our members if the NRC can provide it on or before March 19, 2023, when our Cybersecurity Implementation Workshop begins.

Thank you for considering our request.

If you have any questions concerning this matter, please contact me.

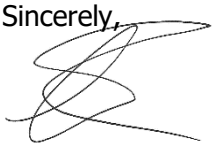
---

[3] See, "Industry Cybersecurity Guidance Adoption Status," by K. A. Manjunatha, T. R. McJunkin, and C. P. Chwasz, September 2022. It is available from DOE at the following URL: https://www.osti.gov/biblio/1892308.

[4] Revision of NEI 08-09 was discussed in a public meeting summarized in, "Summary of October 19, 2022, Public Meeting to Discuss the Nuclear Energy Institute's Project Plan to Revise NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors", November 7, 2022, ADAMS ML22301A099.

[5] NRC letter from James E. Corbett, Chief Financial Officer, to NEI's Richard Mogavero, dated January 17, 2023, ADAMS ML22348A112, responding to fee exemption request dated November 16, 2022 (ADAMS ML22348A112).

Sincerely,



Richard Mogavero

c: NRC Document Control Desk