UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

April 21, 2023

MEMORANDUM TO: Brian M. Yip, Chief
Cyber Security Branch
Division of Physical and Cyber Security Policy
Office of Nuclear Security and Incident Response

FROM: Alexander Prada, IT Specialist (Cyber) Alex Prada Signed by Prada, Alexander on 04/21/23
Cyber Security Branch
Division of Physical and Cyber Security Policy
Office of Nuclear Security and Incident Response

SUBJECT: SUMMARY OF MARCH 29, 2023, PUBLIC MEETING TO DISCUSS THE NUCLEAR ENERGY INSTITUTE'S CYBERSECURITY VULNERABILITY WHITE PAPER

On March 29, 2023, the U.S. Nuclear Regulatory Commission (NRC) held an observation meeting to discuss the Nuclear Energy Institute's (NEI's) white paper, “Remediation of Vulnerabilities Identified in CDAs” (Agencywide Documents Access and Management System [ADAMS] Accession No. ML23072A063), which it submitted to the NRC for review and feedback in support of its planned revision to NEI 08-09, “Cybersecurity Plan for Nuclear Power Reactors." The meeting notice is available at ML23072A361. Approximately 60 participants, including NRC staff, industry representatives, and members of the public attended the meeting.

The white paper supplements existing industry guidance on vulnerability management found in NEI 08-09, Revision 6, Addendum 5, “Cyber Security Vulnerability and Risk Management” (non-publicly available), which the NRC approved for use on August 17, 2018 (ML18226A004). The purpose of this public meeting was for NRC to provide a summary of staff views following review of the vulnerability management white paper for NEI's consideration as it develops Revision 7 to NEI 08-09.

Following introductory remarks from the NRC and NEI, NRC provided an overview of the staff's comments on the white paper. Overall, the majority of the staff's substantive comments fell into two areas. First, the staff disagreed with how the white paper addressed the difference between compromise of the ability to detect a cyberattack and compromise of a CDA itself. The NRC's position is that the reduction (or compromise) of the detection capability of a CDA or the compromise of a system designed to detect (such as a security information and event management system [SIEM]) does not equate to the actual compromise of the system. If a vulnerability is detected on a CDA, the vulnerability management program itself has no direct part in the actual mitigation or elimination of the vulnerability.

CONTACT: Alexander Prada, NSIR/DPCP
301-415-0875

Instead, vulnerability management is a process of identifying, assessing, reporting, and managing vulnerabilities and threats across a licensee's network infrastructure. The actual action of mitigation and elimination comes from other cyber controls that should already be in place per their Cyber Security Plan (e.g., Monitoring Tools and Techniques).

The second substantive point is the understanding of the defense-in-depth (DiD) methodology. The NRC staff stated that vulnerability management is part of DiD and contributes to the layered approach within a licensee's systems. Vulnerability management on its own cannot be considered DiD as many security controls are required to effectively mitigate against cyber threats.

During the Q&A portion of the public meeting, NEI raised questions that NRC intends to address in its written feedback. Some of the questions asked were in relation to indirect CDAs and if they need to be evaluated for vulnerabilities in the same way as all other CDAs. NEI also stated that time to detect and implementing compensatory measures should be considered to evaluate whether to implement vulnerability management on a CDA. They added that if the CDA has no direct impact to a safety or security function, then they believe including the CDA in the vulnerability management program may not be necessary.

During the conversations with NEI at the public meeting, NEI acknowledged it did not adequately explain in the white paper how detection would be credited for the evaluation of vulnerability management for a CDA. The NRC staff indicated that detection alone is not sufficient to justify excluding CDAs from the vulnerability management program.

NRC's next steps is to develop a written response to the NEI's white paper. The response will expand on the presentation given during the public meeting and will provide staff feedback on each section of the paper. The staff anticipates providing its written response to NEI May 2023.

Summary Of March 29, 2023, Public Meeting to Discuss the Nuclear Energy Institute's Cybersecurity Vulnerability White Paper DATE April 21, 2023

DISTRIBUTION:
APrada, NSIR/DPCP/CSB
BYip, NSIR/DPCP/CSB

ADAMS Accession No.: Memo ML23110A724

OFFICE	NSIR/DPCP/CSB	NSIR/DPCP/CSB	NSIR/DPCP/CSB	
NAME	APrada *AP*	BYip *BY*	APrada *AP*	
DATE	Apr 21, 2023	Apr 21, 2023	Apr 21, 2023	

OFFICIAL RECORD COPY