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

December 1, 2021

MEMORANDUM TO: James D. Beardsley, Chief
Cyber Security Branch
Division of Physical and Cyber Security Policy
Office of Nuclear Security and Incident Response

FROM: Gianni Nelson, General Engineer
Cyber Security Branch
Division of Physical and Cyber Security Policy
Office of Nuclear Security and Incident Response

Signed by Nelson, Gianni on 12/01/21

SUBJECT: SUMMARY OF OCTOBER 7, 2021, PUBLIC MEETING TO DISCUSS INSPECTION PROCEDURE 71130.10, "CYBER SECURITY"

On October 7, 2021, the U.S. Nuclear Regulatory Commission (NRC) conducted a partially closed public meeting to discuss Inspection Procedure (IP) 71130.10, "Cyber Security" (Agencywide Documents Access and Management System Accession No. ML21155A209). The purpose of the public meeting was for the NRC staff and industry representatives to discuss the implementation of the IP.

The NRC opened the meeting with an overview of the IP and provided an opportunity for public comment. No participants provided comments or asked questions. Following the Open Session, the meeting moved to a Closed Session to allow for the discussion of sensitive security-related and licensee proprietary information. During the Closed Session, industry representatives discussed specific strategies for ensuring inspection readiness, use of physical protection program, critical digital asset (CDA) security controls, inspection logistics, and perspectives on the differences between protecting information technology and operational technology assets.

During a discussion of the licensee physical protection programs, industry representatives noted the use of this program as part of the defense-in-depth for providing alternate controls. Compliant alternative controls provide defense-in-depth when all five attack pathways are

CONTACT: Gianni Nelson , Cyber Security Branch
301-415-3550

adequately analyzed and mitigated, as applicable. Industry representatives spoke about addressing the area of focus in the next round of inspections as a legitimate method for protecting assets, in addition to establishing an acceptable standard for defense in depth for meeting the intent of Addendum 5 to NEI 08-09, Revision 6, “Cyber Security Vulnerability and Risk Management.” Industry representatives noted that patching without the ability to perform thorough testing may adversely impact safety, security, or emergency preparedness functions.

In the area of CDA security controls assessments, industry representatives discussed vulnerability management assessment implemented through Addendum 5 to NEI 08-09, Revision 6. They noted that vulnerabilities must be exploited through a pathway: physical, logical, wireless, wired, or supply chain. On the issue of inspection logistics, industry representatives spoke on the inspection scope, NRC resource estimate adherence, post-inspection information requests, and inspection logistics. These areas were identified as important because this inspection verifies that the programs meet regulatory requirements and can be consistently implemented across all sites. In the area of information versus operational technology, industry representatives noted that understanding the impact of the systems to the overall risk of the plant will provide nuclear perspectives in an operational environment.