THE U.S. NUCLEAR REGULATORY COMMISSION PUBLIC MEETING SUMMARY

Title: Notice of Meeting with the Nuclear Energy Institute

Meeting Identifier: 20191156

Date of Meeting: November 7, 2019, 09:00 AM to 11:00 AM

Location: The U.S. Nuclear Regulatory Commission
One White Flint North, 11B4
11555 Rockville Pike
Rockville, Maryland 20852

Type of Meeting: Category 2

Purpose of the Meeting:

The purpose of this meeting is to discuss with the Nuclear Energy Institute (NEI), the industry, and the public NEI's White Paper titled, “Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Emergency Preparedness Functions,” dated October 2019.

General Details:

The U.S. Nuclear Regulatory Commission (NRC) staff held a public meeting with the NEI. The meeting started at 09:00 a.m. and ended at 11:00 a.m. There were 13 NRC staff members, 4 NRC contractors, and 8 industry representatives present in the room. On the phone, there were three NRC staff members, six industry representatives, three members representing private companies, and one member of the public. Mario Fernandez from the Office of Nuclear Security and Incident Response began the meeting with introductions of NRC management and staff, and industry representatives present in the room. Participants on the phone were not introduced, in the best interest of time. However, remote participants were provided the opportunity to send their information via e-mail to be entered on the record.

The NRC management addressed the attendees by providing an overview of the NRC efforts (NRC Cyber Security Assessment Action Plan Presentation) to enhance and improve the NRC Cyber Security Oversight Program by utilizing more risk-informing approaches. The management also thanked the industry for their initiative to get involved and working with the NRC by updating and revising NEI’s cyber security guidance. The industry’s initiatives are in parallel with the NRC efforts and the emergency preparedness (EP) area is one of the six areas considered for enhancements and updates.

Summary of Presentations:

Following the introductions, James Beardsley, Chief, Cyber Security Branch, provided background on the NRC staff efforts to improve the NRC Cyber Security Oversight Program. He discussed the program assessment conducted in the spring of 2019 and the development of the NRC Cyber Security Action Plan to address the areas highlighted in the assessment. The following areas of focus are detailed in the action plan:

- Clarifying Program Definition and Terms
- Critical Digital Asset (CDA) Determination:
    - EP
    - Balance-of-Plant (BOP)
    - Security
    - Safety-Related and Important-to-Safety
- CDA Assessment Best Practices
- CDA Controls (Near Term)
- CDA Controls (Long Term, industry's Low Priority)
- Cyber Inspection Oversight Program Following Full Implementation

Following Mr. Beardsley's presentation, Bill Gross, Director Incident Preparedness at NEI, thanked the NRC for getting the industry involved and for providing the opportunity to discuss the efforts to improve the NRC Cyber Security Oversight Program. He mentioned this is the beginning to address the lessons learned (from the inspections already completed) by the NRC and the industry. Mr. Gross discussed the history of the cyber security program (post 9/11 until now). He mentioned that the industry has identified several areas where clarity and efficiency can be attained by revising NEI guidance. Mr. Gross mentioned the industry is focused in achieving two objectives. First, he emphasized that as the industry is working through the changes of NEI 10-04 and NEI 13-10, the public's health and safety will be maintained by ensuring the industry continues to meet the NRC requirements of Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54. The changes proposed will ensure digital components associated with the EP functions will be analyzed to determine whether a cyber attack would adversely impact the ability to accomplish the EP functions. Where alternate means or alternate methods are available, and the licensee can demonstrate a cyber attack would not adversely impact the licensee's ability to maintain the EP functions, the licensee will not designate those EP digital assets as CDAs. He noted that through the change management processes, the licensee will continue to monitor changes to those EP digital assets or systems.

Second, Mr. Gross noted that the industry wants to ensure the alternate means or alternate methods are credited and will be properly monitored. Changes to the emergency plan will be evaluated to ensure that there are no adverse impacts to the capability of the EP digital components to perform their function. In addition, the industry will ensure the alternate means or methods can be used and still meet the emergency plan timelines.

Finally, Mr. Gross noted that the industry would evaluate their proposed changes to ensure that the terminology is consistent with similar terminology in the emergency plan and associated processes. Mr. Gross noted that the outcome of the industry's effort will ensure that licensees' programs will continue to adequately protect the public's health and safety, EP CDAs are protected in accordance with the cyber security plan, and other digital assets will be protected under the corporate cyber security programs. He thanked the NRC for the efforts in the initial review of the document and looks forward to discussing the NRC staff's feedback.

David Neff, Principal Regulatory Engineer at Exelon, provided positive remarks about the efforts and the initiatives between the NRC and the industry, and the ongoing activities to resolve the lessons learned and the areas of concern identified for improvement. One area of concern moving forward is communicating these changes to the NRC inspectors and to the industry. NEI will communicate guidance changes to the licensees once the changes are approved for use by the NRC. He also mentioned looking at implementing other approaches based on performance testing to achieve effectiveness and efficiency in the oversight program.

NRC Staff Feedback on the Proposed Industry Guidance:

Mario Fernandez, Cyber Security Specialist at the NRC, continued the meeting and stated that the main purpose of the meeting was to provide an opportunity for the public and stakeholders to provide feedback regarding the NEI's White Paper titled, “Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Emergency Preparedness Functions,” dated October 2019.

Mr. Gross then described the purpose and scope of the document. He mentioned the architect of the proposed changes was Matt Coulter (on the phone) and any technical questions should be directed to Matt.

Mr. Fernandez opened the questions and comments portion of the meeting beginning with the NRC staff. The following questions and/or comments were received:

- Normalize the language in the documents by aligning terminology in NRC EP regulations, NRC guidance, or other documents (e.g., backup means or compensatory measures) and avoid introducing ambiguous or undefined language in the guidance (e.g., independent alternate method vs. means).
- Equipment being taken credit for must be identified in the emergency plan. This will ensure clarity during inspections. It was noted that alternate means or compensatory measures included in the emergency plan have already been approved by the NRC. Therefore, licensees should align the language in the CDA assessment description with the language in the emergency plan.
- Concern was raised regarding detection of compromised digital indicators. If operators relied upon digital indicators to make decisions, can the operator detect the compromise of digital indicators? Does the operator have an alternate non-digital means to ensure the function can be appropriately accomplished?
- There must be a way to timely detect the primary method has been compromised to ensure operators use the alternate method to accomplish the EP function.
- For clarification, even if the function can be performed with alternate means, this approach solely does not remove the EP CDA from being a CDA. If the function can be performed with alternate means, the asset must be further evaluated to ensure other requirements are not violated. For instance, a cyber security requirement may be violated due to connectivity to other CDAs.

Matt Coulter addressed some of the questions and concerns raised by the NRC staff by stating that the industry will ensure the alternate method is defined in the licensee’s emergency plan. In addition, there will be adequate detection of compromise or failure of the digital asset that would drive licensees to use the alternate method in the time required to fulfill the EP function. These comments reflect the need to clarify the language in the document as it may not be clear or obvious.

Mr. Coulter noted the criteria or the filtering process to remove EP digital assets from the CDA list entails several steps. One of those steps is to evaluate the asset for connectivity and other potential conflicts within the cyber security program.

Mr. Neff asked for clarification about the cyber security control periodicity conflicting with the EP requirements of dose assessment software. The NRC staff answered his question by clarifying

that licensees may take credit for security controls implemented and the verification periodicity at the periodicity established by the EP requirements.

Shana Helton, Director, Division of Physical and Cyber Security Policy, took the opportunity to address the industry by proposing piloting the guidance and the use of tabletops to test the proposed changes and to ensure the conflicts and challenges are resolved before rolling out the revised guidance associated with the EP digital assets.

The NRC staff also raised the concern whether the proposed changes would allow a licensee to descope all its EP digital assets from being CDAs. Mr. Gross answered the staff's concerns by stating that it is very difficult to answer with certainty this outcome. However, it may be possible that a licensee may not have any EP CDAs if most of the licensee's systems are not digital. He re-stated that guidance and the change control process require licensees to evaluate changes to the emergency plan to ensure CDA determination is performed correctly.

Eric Lee, NRC Cyber Security Specialist, raised a concern regarding the protection of an EP CDA that causes an adverse impact to the EP function. The NRC expects any CDA that causes an adverse impact to the EP function to be protected as a direct CDA per the NEI 13-10 process. The document must include this clarification because the new scoping methodology will identify those CDAs where a cyber attack could adversely impact the licensee's ability to perform the EP function.

Mr. Coulter addressed Mr. Lee's concern and asked if Mr. Lee was referring to the criteria in the NEI 13-10 process for indirect CDAs. Mr. Lee noted that the new process could potentially re-classify an EP CDA from the indirect category to a direct CDA category. This question/concern will be addressed during a tabletop or implementation discussion meetings in the future to ensure there are no gaps or flaws introduced in the guidance.

Bob Kahler, NRC Branch Chief, Policy and Oversight Branch, mentioned the importance of associating the language in the cyber security guidance with language in the emergency plan or EP procedures as this will also help with 10 CFR 50.54(q) reviews, particularly when the licensee is taking credit for compensatory measures to meet cyber security requirements.

Mr. Kahler also noted two concerns:

- The scoping methodology in the guidance document has a clear path for determining what is not an EP CDA, but it does not provide clarity about determining what is an EP CDA and the required protection. Mr. Neff addressed this question and agreed the document needs to be clear regarding the identification of an EP CDA and the required protection in accordance with the NEI 13-10 process.

- CDA identification and the nexus to NUREG 0654, "Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants (NUREG-0654/FEMA-REP-1)," currently under revision, Table B2 Rev. 2, "Staffing requirements for an Emergency Response Organization," has been issued and there is a new requirement for licensees. For those licensees that have identified EP CDAs, the new staffing requirements should include having an Information Technology person respond in a certain amount of time in the event of a cyber attack to an EP CDA.

Mr. Lee commented that record retention and supporting technical documentation must be maintained for those digital assets that will no longer be EP CDAs for NRC oversight in the future.

Public Participation Themes:

Pia Jensen, a member of the public, asked several questions that were outside the scope of the guidance documents being addressed at the public meeting. These questions will be answered in a separate forum.

Shonique Miller, Entergy, asked the following questions:

- Will normalizing the definition of terms in the guidance document have any impact on the already performed NEI 13-10 assessment and process? The guidance document indicates not to re-perform the alternate means determination or the already assessed EP CDAs. Mr. Coulter noted that changes to guidance should not require a licensee to re-perform past assessments.

- Will these changes require a license amendment request or will this have to be approved under the 10 CFR 50.54(p) analysis? Mr. Coulter noted that the proposed changes do not impact the licensee's cyber security plan and thus would not require a licensing change.

- Will examples be provided in the guidance document, specifically if a digital asset can be remediated it may not be an EP CDA? Mr. Coulter noted that it was not planned or intended to include examples in the white paper. However, in NEI 13-10 there are some examples in the EP section that will need to be removed, updated, or revised to reflect the new process.

- The flowchart in the guidance document needs to be corrected in the BOP section. There should be a "no" instead of a "yes." Mr. Coulter agreed that this will be corrected in the document.

- For defense-in-depth, what does it mean for licensees now regarding the defense-in-depth for level 2? Will there be any guidance forthcoming or will this be addressed by each licensee? Mr. Gross addressed the question about defense-in-depth and explained that when the changes were reviewed, the working group did not identify the proposed changes would cause holistic changes to be made; however, a holistic change may be site-specific.

There were no further questions from participants on the phone.

Action Items/Next Steps:

Mario Fernandez summarized the next steps as follows:

- The NRC and NEI will continue the dialogue and discussions to ensure the proposed changes improve the NRC cyber security programs and are within the regulatory framework.

- Adopt a more risk-informed approach to the CDA determination and protection that is aligned with NRC EP requirements and EP plans. Specifically, normalization of the terminology to harmonize the NEI cyber security guidance with the EP requirements and the EP plan.

- Comments and concerns from the stakeholders will be evaluated and addressed to ensure the proposed changes do not create unintended consequences. Any additional comments received after the public meeting will be available to the industry, so the comments can be evaluated and addressed appropriately.

The industry will continue pursuing the endorsement of the white paper pending the posting of the meeting summary to address all the questions and concerns raised during the public meeting. The meeting was adjourned by Mario Fernandez at 11:00 a.m.

Attachments:

Title	Organization	ADAMS Accession Number
11/07/2019 Notice of Meeting with the Nuclear Energy Institute (NEI)	NRC	ML19296C717
NEI White Paper Proposing Changes to NEI 10-04 and NEI 13-10	NEI	ML19295D806
NEI 10-04, Revision 2, "Identifying Systems and Assets Subject to the Cyber Security Rule"	NEI	ML12180A081
Review of NEI 10-04, "Identifying Systems and Assets Subject to the Cyber Security Rule," Revision 2, Dated July 2012	NRC	ML12194A532
NEI 13-10, Revision 6, "Cyber Security Controls Assessment"	NEI	ML17234A615
Public Meeting Action Plan Presentation	NRC	ML19323G000

List of Public Meeting Attendees
November 7, 2019

Name	Organization
Charity Pantalo	NRC
Brian Yip	NRC
Michael Brown	NRC
Ralph Costello	NRC
Eric Lee	NRC
Juris Jauntirans	NRC
Robert Kahler	NRC
Todd Smith	NRC
Ismael Garcia	NRC
James Beardsley	NRC
Mark Lombard	NRC
Shana Helton	NRC
Joe Cristiano	OASIS (NRC Contractor)
Bill Johns	OASIS (NRC Contractor)
Tim Marshall	OASIS (NRC Contractor)
Kimberly Edwards	OASIS (NRC Contractor)
James Andersen	EXCEL Services Corporation
Stephen Flickinger	Exelon
Nathan Faith	Exelon
David Neff	Exelon
Brian Young	FENOC
William Gross	NEI
Richard Mogavero	NEI
Jim Shank	PSEG

List of Public Meeting Callers
November 7, 2019

Name	Organization
Eric Martinez Rodriguez	NRC
Kim Lawson-Jenkins	NRC
Dave Werkheiser	NRC
Tony Lowry	AMEREN (Callaway Energy Center)
Larry Nicholson	Certrec
Jana Bergman	Curtiss-Wright
Matt Coulter	Duke Energy
Jan A. Geib	Dominion Energy (V.C. Summer Nuclear Station)
Keith Drewke	Florida Power & Light (Turkey Point Nuclear Plant)
Pamela Frey	Talen Energy (Susquehanna Steam Electric Station)
Eugene Keller	Talen Energy (Susquehanna Steam Electric Station)
Dave Feitl	Xcel Energy
Pia Jensen	Member of the public
Shonique Miller	Entergy