U.S. Nuclear Regulatory Commission Public Meeting Summary

Title: Notice of Virtual Meeting to Discuss Changes to Emergency Preparedness Digital Assets Cyber Security

Meeting Identifier: 20191156

Date of Meeting: August 06, 2020, 10:00 AM to 3:00 PM

Location: Virtual Meeting via WebEx

Type of Meeting: Category 2, partially closed

Purpose of the Meeting(s):

The purpose of this meeting is to discuss with the NEI, the industry, and the public the implementation of 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 March 2020.

General Details Open Session:

The NRC staff held a virtual public meeting with the NEI, the industry, and the public to discuss the implementation of the guidance in the NEI's white paper. Mario Fernandez from the Cyber Security Branch, Office of Nuclear security and Incident Response (NSIR) began the meeting by thanking all the participants, attendees, and panelists. Only the industry panelists and NRC management were introduced. Participants online and on the phone were not introduced, in the best interest of time. Participants information will be entered on the record from the event registration. After the introductions, instructions for the format and procedures for participating in the open and closed sessions of the meeting were provided.

Next, Brian Thomas, Deputy Director, Division of Physical and Cyber Security Policy, NSIR, made his opening remarks. He thanked the attendees and the NEI for participating in the efforts to improve guidance for the cyber security oversight program. Mr. Thomas mentioned the efforts in developing guidance and policy clarification documents between the NRC and the Industry that have been taking place over the past 10 years to stand up the cyber security oversight program. A key example of the ongoing coordination between the NRC and the NEI is the proposed changes to NEI guidance for identifying and protecting digital assets (DAs) associated with Emergency Preparedness (EP) Functions. This public meeting and subsequent workshops will help the NRC staff and the industry to understand guidance implementation and oversight of subsequent changes, and it will also help the staff to identify any challenges or gaps in implementing the guidance in the white paper.

Next, James Beardsley, Chief, Cyber Security Branch, NSIR, provided background on the NRC staff’s efforts to improve the NRC Cyber Security Oversight Program. He provided an overview of the cyber security oversight assessment the staff conducted in 2019 and mentioned the assessment included all aspects of the program. As a result of this assessment, the staff provided recommendations to management and developed a cyber security action plan to reevaluate certain areas for potential improvements. The NRC and the industry have come together in several areas and emergency preparedness, the topic of this meeting, is the first

area that the NRC has completed the review of and provided feedback to the industry on the methods for implementing the changes the industry has proposed. Our goal today is to review the process the industry will use to evaluate EP assets, discuss the methods the industry will use to implement those changes, and how the NRC staff will view those changes in the oversight capacity. This portion of the meeting will be held in a closed session because there are licensee's specific implementation details that are not proper for public discussion and should be conducted with participants who have a need to know. Mr. Beardsley also thanked all the presenters and the attendees for their participation in the meeting today.

Following Mr. Beardsley's remarks, the NEI represented by Bill Gross and Rich Mogavero made opening remarks. First, Mr. Gross thanked the NRC for hosting this engagement with the industry because this forum is valuable for effective implementation of revised guidance. This effort is reflective of two of the NRC principles of good regulation, the first being efficiency. Mr. Gross recognized the efforts by the industry and the NRC in working together to complete the review and address the comments of the proposed changes in a timely manner despite the current pandemic situation. He noted that the current NRC-approved NEI guidance was effective but could be more efficient. The revised approach addresses efficiency issues and ensures that licensees continue to maintain adequate protection allowing utilities to utilize an appropriate amount of resources focusing on cyber security of other plant DAs. Under the principle of clarity, the revised guidance is not only clear, but it is also consistent with the underlying objectives of ensuring that emergency preparedness functions are not adversely impacted by a cyber attack.

Mr. Mogavero, Senior Project Manager at NEI, also thanked the NRC and the industry for meeting today regarding the guidance for EP DAs. The industry's and the NRC's understanding of the cyber aspects and EP protection has evolved since the rule was issued. From 2010 to 2013, NEI issued guidance to licensees for identification and protection of DAs. Licensees identified a wide range of EP related DAs as critical digital assets (CDAs). The industry has learned over time to perform assessments using the NEI 13-10 methodology that a cyber attack would not adversely impact the ability to accomplish the EP function. However, there was no guidance that provided a clear methodology to remove those assets from being called CDAs. The recent proposed revisions correct this. The enhancement of both documents will provide criteria for identifying the right DAs while ensuring the requirements of 10CFR 73.54 (b)(2) are met. Lastly, the program remains effective. The proposed changes in NEI 10-04 and 13-10 do not constitute a reduction in the effectiveness of the cyber security plan (CSP). The intent of the changes is to leverage the work that has already been performed which demonstrates how the EP functions are fulfilled regardless of compromise to the associated digital equipment used as one of the methods to perform the EP function.

Next, Mr. Fernandez explained that efforts to enhance the cyber security oversight program began with the NEI proposing revisions to previously approved NEI cyber security implementation guidance. The first effort began with the proposed revisions described in the NEI 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. This was the first revision and the first attempt to improve the NEI guidance. On November 7, 2019, the NRC conducted a public meeting with the NEI representatives, the public, and other stakeholders to discuss the changes proposed in the NEI white paper. Thereafter, the NRC clarified the feedback from the meeting with the NEI and industry representatives. Details of the public meeting are documented in the "Public Meeting Changes to NEI 10-04 and NEI 13-10 Summary dated, Nov 7, 2019," ADAMS Accession # ML19331A409. The NEI addressed all the comments provided and re-submitted its revised

white paper to the NRC for review and approval. After conducting a thorough review of the NEI white paper, the regulations, NRC-approved guidance, and the statements of consideration for the NRC Cybersecurity Rule, the NRC has concluded that the proposed changes in the NEI white paper, "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Emergency Preparedness Functions," dated March 2020, are consistent with NRC-approved implementation strategies or approaches described in NRC Regulatory Guide 5.71, "Cyber Security Program for Nuclear Facilities," ADAMS Accession # ML090340159 and in NEI 08-09 Rev. 6, "Cyber Security Plan for Nuclear Reactors," ADAMS Accession # ML101180437 to meet the requirements of 10 CFR 73.54.

General Details Open Session:

Next, Matt Coulter discussed the background and development of the NEI white paper. The NRC staff, the industry, the public, and other stakeholders were given the opportunity to ask questions. There were no questions. Mr. Fernandez ended the open session and provided instructions for the closed session of the meeting. Questions or comments related to the open session can be sent to Mr. Fernandez at mario.fernandez@nrc.gov.

General Details Closed Session:

The closed session of the meeting started at 11:15 a.m. and ended around 2:45 p.m. Mr. Fernandez began the session by going over the format and procedures for this part of the meeting. Then, he proceeded by turning the meeting over to industry for the presentation of the topics related to the NEI guidance. A summary of the topics presented is included below.

Summary of Presentations:

Mr. Coulter provided details about the background and development of the NEI white paper "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Emergency Preparedness Functions, Dated March, 2020". Mr. Coulter noted the criteria or the filtering process to remove EP DAs from the CDA list entails several steps. One of the most important steps is to evaluate the asset for connectivity and other potential conflicts within the cyber security program. There were no questions related to the topic presented.

Next, the panelists presented three examples of EP assets that were re-evaluated and would be re-classified using the guidance in the NEI white paper. These examples described the process, the methodology, and the basis that the industry could use in accordance with the criteria in the revised guidance.

Feedback on the Implementation Strategy of NEI's White Paper Guidance:

For the first example, the industry described a backup system that will be re-classified as an EP DA because:

- The primary method is an onsite monitoring system. Other sites or a third party can assist since the procedures are similar. The third party is an independent contractor. This system is a backup system to the primary system as required by the Emergency Plan (EPlan).

- Relying on offsite capabilities as a backup and the monitoring that must be done requires collecting samples and then further testing these samples by other sites, impact on the timeliness of the availability to analyze those samples and adequately assess the conditions of the site for a declaration is important.

- There is basis for emergency action level classifications, even with the capabilities onsite, the samples analysis could take several hours. Does this impact your capability? The inspectors will be evaluating this very closely. Is this impacted by the alternate method? From the cyber perspective, consider the timeliness of the ability to perform that function.

- Ensure changes to the EPlan follow the 50.54(q) process under EP and when DAs are determined to be non-CDAs based on initial reviews. Changes to the EPlan and emergency preparedness implementation procedures could adversely impact the cyber security elements reviewed. It is important to stress that when changes are made using the 50.54(q) for EP involving DAs the cyber security elements are reviewed again.

- When the system is down, and its condition is entered in the corrective action program is there a notification to the shift manage or the emergency response organization (ERO)?

- Other sites in the fleet assist with this system. Data is sent via courier to multiple sites. Sites are within proximity of each other and have the same procedures. The industry needs to verify If this capability is tested. Also, if the contractor is needed, there is a 24 x 7 response for the analysis. The contractor's capability is tested during drills.

- The questions associated with can the cyber compromised be detected in time? There are two references to detecting a cyber compromise and this question relates to all 3 examples. What amount of functional testing is to be used, how regular, and what frequency is considered acceptable necessary to answer this question as "met". The intent of the white paper is to reflect that the existing methods or means for detection that are currently outlined in the emergency plan or implementing procedures are adequate regardless of how that digital asset fails.

- If the alternate method is also a digital device or digital means are credited to perform the function, those assets also have to be evaluated similarly to your primary digital means to prove how the criteria is met and if they are interconnected they may not the criteria unless properly controlled and protected from one another.

- Connectivity alone is not a sole criterion for CDA classification. An evaluation must be performed to determine if the interconnected CDAs are adequately protected against a cyber attack. This is very similar from the guidance in approved NEI 10-04. Connectivity along does not automatically make it a CDA. Other considerations must be considered such as the protections around the device, how they interact, and the processes associated with it.

- EP DAs vulnerabilities will not be addressed through the cyber security oversight process (NEI 08-09 Rev. 6, Appendix E Section E.12), but it will be addressed through internal or corporate processes.

- ERO personnel are trained to use alternate methods if the primary methods are not available. There are checklists that help determine if the primary methods are not available, then staff will use the alternate methods that are available. The training or the procedure that the ERO personnel uses to perform this activity will be made available to the inspectors.

- Licensees need to make sure that future assessments include the level of detail necessary for an independent reviewer to arrive at the same conclusion as to what is written on the assessment. References to drawings, procedures, checklists, and other documents must be included in the assessments.

- Daily checks and other checks provide a reasonable assurance the asset can perform its function. The system manager or the subject matter expert monitor the system. The important thing is to detect the exploitation of a vulnerability.

- Defense-in-depth protective strategies will be maintained through routine testing of these assets to ensure the capabilities to detect, respond to, and recover from cyber attacks. This is an alternate system so any changes in the future will have to be managed. The guidance provides direction regardless of a cyber attack whether the EP function can be fulfilled. If the answer is no, then the asset becomes a CDA and then cyber security protections must be put in place to be in compliance with the rule.

For the second example, the comments and questions are noted below:

- There are different operational checks identified for this system and the system discussed previously. Keep in mind that those checks are being credited to provide reasonable assurance of the potential timely detection of the loss of function of that equipment. If the daily checks are removed, the monthly, quarterly checks do not provide that reasonable assurance.

- The licensee staff is required to train on the use of the alternate method, and this is demonstrated during drills and exercises. For example, during drills and exercises licensee staff is required to use the checklists for their position and demonstrate the procedures are being followed. Also, equipment failure injects are used to verify the ERO personnel know how to use these alternate methods. Routine activities performed daily do not require testing.

For the third example, the comments and questions are noted below:

- With the increase use of technology notifications are being done electronically which is significantly different using computers and the Internet and timely detection is the key to give credit for identification for the loss of the function. Is that timely detection again that becomes critical.

Next, industry representatives described the change management and the 50.54(p) processes, the basis required to be documented to make changes in the CSP, and other activities associated with the implementation of the guidance in the NEI white paper.

For the presentations above, the comments and questions are noted below:

- Although there is no regulatory requirement for most cases, some of the re-classified assets will be protected by the corporate or site cyber protection program.

- There were further comments and discussions regarding whether a device that performs the function must be protected under the rule and questions about the critical group requirements. However, the revised screening methodology that applies to EP devices only states the EP function must be protected and not the function of the device. Further clarification and discussions will be provided via the industry's forum.

- It should be noted that this system is not only associated with EP functions. It is important to note that this system may perform other functions and that system must be assessed accordingly.

- The industry needs to verify if this system is identified in security procedures or the security plan.

Action Items/Next Steps:

Mario Fernandez summarized the next steps as follows:

These discussions have been very informative to the NRC and I hope that our comments and questions provide positive feedback to the industry as the licensees continue with the implementation of the proposed changes in the NEI white paper titled "Guidance for Identifying and Protecting Digital Assets Associated with Emergency Preparedness Functions," dated March 2020. Based on these discussions, the NRC and the NEI will continue working to:

- Improve the effectiveness and efficiency of the NRC cyber security oversight program while maintaining program effectiveness to protect against cyber attacks up to and including the DBT.

- Maintain a risk-informed approach to the CDA determination and protection that is aligned with NRC EP requirements and licensees EPlans.

- Not create unintended consequences. Comments and concerns from the stakeholders will be evaluated and addressed to ensure ambiguities and unclear language are clarified in the final revision of the NEI 10-04 and NEI 13-10 guidance when submitted to the NRC for final review and approval.

- Identify implementation challenges or gaps and to further clarify guidance ambiguities in the future revision of the EP CDA determination and protection guidance when submitted for NRC review and approval.

Attachments:

Title	Organization	ADAMS Accession Number
08/06/2020 Notice of Virtual Meeting to Discuss Changes to Emergency Preparedness Digital Assets Cyber Security	NRC	ML20218A285
NEI White Paper Proposing Changes to NEI 10-04 and NEI 13-10	NEI	ML20126G492
Response To NEI White Paper, "Changes To NEI 10-04 And NEI 13-10 Guidance For Identifying And Protecting Digital Assets Associated With Emergency Preparedness Functions," Dated March, 2020	NRC	ML20129J981
NEI Guidance for Identifying and Protecting Digital Assets Associated with Emergency Preparedness Functions Presentation (Internal Use Only)	NEI	MLXXXXXXX

List of Participants
August 6, 2020

Industry Representatives

Adam Driscoll ++
Ali Corl ** ++
Barry Westreich **
Brian Loose
Brian Miner *
Brian Young ++
Chadwick Vinje
Chance Siri **
Chris Ambrose **
Dan Butor **
Dan King
Dave Draghi
David Costley
David Neff ++
David Wroblewski
Denny Smith **
Desiree Wolfgramm
Don Robinson **
Edie Boyer **
Eric Roehrig **
Eugene Keller
Galen Riley
Harry Willetts
Heather Pickard
Jack Kostreba
James Hazel
Jan Geib
Jana Bergman
Jason Baron
Jason Castro
Jason Davis
Jason Taken **
Jerry Mills **
Jesse Pitts **
Jim Shank
Joel Manning
Joseph Witts
Keith Kauffman **
Kevin Deyette
Kevin Fontenot
Kevin Garpne
Kevin Sykes **
Kristen Howell
Kurt Hofmann
Lillie Winckowski **
Lincoln Goede **
Manu Sharma ** ++
Mark Denton
Marvin Hearl
Mary McCague **
Matt Cha *
Matt Coulter ++
Matthew Morgan
Miranda Wolf **
Nathan Faith
Nathaniel Mlady
Richard Mogavero
Richard Mothena
Robert Goley **
Robert Koch
Robert Stubbs
Roderick Gunther
Scott Greenslit **
Shonique Miller
Stacy Baskin
Stephen Flickinger **
Steven Sullivan
Timothy Mabry
Tony Lowry ++
Wesley Lottes
William Gross

NRC Representatives

Steven Alferink
Alan Konkal
Alex Prada
Brandon Pinson
Brian Thomas
Brian Yip
Casey Priester
Charity Pantalo
Cynthia DeBisschop
Eric Lee
George Hausman
Glenn Dentel
Greg Pick
Gregory Hansen
James Beardsley
Joe Cristiano **
Juris Jauntirans
Kim Holloway
Kim Lawson-Jenkins
Kimberly Edwards
Mike Brown
Nnaerika Okonkwo **
Richard Skokowski
Sam Graves
Scott Shaeffer
Shiattin Makor
Shyrl Coker
Tim Marshall
William Johns
William Monk

Other Stakeholders

Gary Locklear
Alex Bond **
Troy Burnett **
Robert Cole **
Dewey Coulon **
Rory Gunther **
Roosevelt Holmes **
Thomas Novotny **
Joseph Orlando **
Diana Tragar **
Andrew Zillins **

Industry panelist ++
Attended both sessions
Attended open session only *
Attended closed session only **