Closed Public Meeting Summary
2023 Cybersecurity Inspections Lessons Learned
February 15, 2024

On February 15, 2024, the U.S. Nuclear Regulatory Commission (NRC) held a public meeting to discuss lessons learned and trends identified from the 2023 cybersecurity inspections conducted using Inspection Procedure (IP) 71130.10, “Cyber Security,” dated January 2022 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML21155A209); the meeting notice (Enclosure 1) is available in table 1 below. The hybrid meeting was facilitated in-person with attendees at NRC headquarters and virtual attendees joined via Microsoft TEAMS. There were 9 in-person participants and 103 virtual attendees comprised of NRC staff, industry representatives, and members of the public (see Enclosure 4 for a complete list of attendees).

The meeting addressed security-related information regarding licensees’ cybersecurity plans and implementation methods and was limited to participants with a need to know; the meeting also provided members of public an opportunity to ask questions and provide feedback. The objectives of the engagement were to discuss: 1) the cybersecurity baseline inspection activities conducted during calendar year (CY) 2023; 2) lessons learned and trends from the 2023 cybersecurity inspections; 3) any actions needed to ensure efficiency and effectiveness of future inspections.

Following brief introductions and opening remarks, the NRC staff lead the discussion with a presentation (Enclosure 2) which focused on the IP objectives and requirements, CY 2023 top trends for more-than-minor violations and cross-cutting aspects, inspection observations, lessons learned, insights to the potential causes, and next steps to increase efficiency the program enters the next biennial inspection cycle. Regarding the lessons learned the NRC staff provided the following: 1) the one-week inspection is resource intensive, presents many challenges, and results in a tight inspection schedule for the NRC and the licensees; 2) inspectors have observed that the best performing sites and well-maintained cybersecurity programs have strong support from senior management; 3) documentation reviewed during inspections does not reflect the whole story (who, what, when, & why) and security control implementation is not reflected in the paperwork; 4) inspectors have also observed some licensee staff lacked experience with regulatory requirements, background, and guidance related to the implementation of the cybersecurity program.

To inform the industry and the public of the next steps the staff are taking to increase efficiency, the NRC staff discussed the working group the agency established to evaluate alternate IP frequencies and team composition. Staff added that the working group will develop recommendations for management consideration and any proposed changes to the IP will be discussed during a future public meeting. Following the NRC presentation, staff clarified a question regarding the number of cybersecurity Green findings which current data shows approximately 30 Green findings per 1000 hours for the full biennial inspection cycle.

NEI’s presentation (Enclosure 3, non-public at NEI’s request) focused on providing industry’s perspective on the IP, significance of findings, and industry's insights regarding the cybersecurity inspection program. NEI stated that based on recent polling, inspectors are evaluating all five inspection requirements based on unusual circumstances, or special

considerations versus the nominal 4 and added this may contribute to why it's challenging to complete inspections in a timely manner. NRC staff responded by stating, in concert with the information presented during NRC's presentation on this topic, regional inspectors indicated this is a result of how the IP is written and the requirements have overlap; NRC staff acknowledged this may be an area of the IP that could potentially be considered for enhancement in the future and captured as an item for programmatic discussion.

Regarding the topic of sample selection, a licensee representative added that licensees have noted scope creep where subsystems that were not included as part of the request for information (RFI) for selected samples are inspected based on the dependence to the selected sample system. The representative of industry added this is key because the additional subsystems often introduce an issue where the subsystem owner may not be available for the inspection resulting in delays; and closed by stating that industry anticipates the NRC action to address aligning the IP with RFI 2. NRC staff responded by stating the intent of the RFIs are to ensure the inspection team has the required documentation and information needed to conduct the inspection and added asking clarifying questions is encouraged regarding sample selection.

NEI then discussed their perspective of the significance of findings, by stating the current IP seems to give inspectors limited flexibility when assessing issues against the cybersecurity plan, even if there is very little, no safety, or no security vulnerabilities identified. The significance determination process (SDP) does not allow an offramp if a performance deficiency is identified and whether it should be a minor violation or an observation. Furthermore, if a performance deficiency is identified the evaluation starts in the Green realm and then the determination is made whether the performance deficiency will be minor or more than minor. To address these concerns which may reduce the NRC and licensee burden, NEI offered the following insights: 1) consider a definition for cybersecurity margins to the upcoming revision of NEI 08-09, Rev. 7; 2) continue to update the minor/more-than-minor cybersecurity examples; 3) incorporate the principles of the Very Low Safety Significance Issue Resolution process. The NRC staff asked NEI to clarify the meaning of offramp to ensure that staff understood the concern. This led to considerable discussion about requirements, implementation of controls, performance deficiencies and how they are evaluated for significance. The NRC staff also stated that perhaps there is a disconnect in NEI's understanding of the terminology, language, and an understanding of the SDP process. The NRC staff annotated this as a topic to potentially engage with industry to further the discussion in the future.

The last topic of the NEI presentation, a licensee representative provided perspectives on improving the overall efficiency and effectiveness of the IP. In summary, the industry believes that a triennial inspection cycle would allow a year runtime to remediate findings, provide an accurate snapshot of the program, and allow time to adjust to changes.

Finally, during the questions session, one member of industry asked if any of the future inspections would be scheduled to exit after the Friday of the inspection? Specifically, if the inspection team plans to notify licensees during the entrance meeting, they would not exit on Friday. A Region 2 inspector commented that during the entrance meetings he has led in the past, he briefs the licensee inspection team that every effort would be made to exit on time; however, if there are specific unresolved questions and issues the inspection team would need to resolve those issues prior to exiting. NEI also commented that during this biennial inspection cycle, industry was aware that given the scope and fast pace of the inspection some concessions were needed and do not consider an inspection having a virtual entrance meeting

the Thursday before the scheduled inspection week or a virtual exit meeting the Tuesday following the scheduled inspection as an extended inspection. The NRC staff noted the question to inquire about this topic with regional inspectors.

In closing, NEI expressed their appreciation to the NRC as well as the industry and all who supported the public meeting. NEI expressed there is a lot of work to do on the industry side in terms of understanding the status of our programs and believes there is an opportunity for the NRC to evaluate the IP, RFIs, and the approach of the biennial inspection process for improvements. The NRC staff concluded the meeting by acknowledging the concerns raised by industry representatives, thanking the participants for an engaging discussion, and noting the need for future discussions and engagement of some of the issues (as noted in table 2) as a continuing effort to enhance the program.

Meeting Point of Contact: Tammie Rivera, NSIR/DPCP/CSB

Table 1. List of Enclosures

Enclosure #	Title	ADAMS ML
1	*2023 Cybersecurity Baseline Inspections Lessons Learned Public Meeting*	ML24023A693
2	*NRC Presentation - CY23 Cybersecurity Inspections Lessons Learned - Closed*	ML24043A087
3	*NEI Presentation - Cyber Insp Lesson Learned*	ML24065A171 (**non-public**)
4	*2023 Cyber LL Meeting (Closed) - Attendance Report*	ML24066A069

Table 2. Summary of Action Items

#	Action Items	Engagement
1	Inform industry of agency's decisions regarding the working group efforts	Future public meeting
2	Re-evaluate the inspection requirements of the IP for potential clarification	Initial - internal review
3	Re-evaluate the IP to ensure alignment with RFI 2.	Initial - internal review
4	Follow-up discussion regarding the significance of findings	Future public meeting
5	Triennial inspection cycle consideration	Initial - internal discussion