PUBLIC MEETING SUMMARY REGARDING LESSONS LEARNED DURING MILESTONES 1-7 CYBER SECURITY INSPECTIONS

On December 6, 2016, the U.S. Nuclear Regulatory Commission (NRC) staff held a public meeting at NRC Headquarters in Rockville MD to discuss lessons learned by the NRC and industry during Milestones 1-7 cyber security inspections and to discuss planned actions for upcoming Full Implementation cyber security inspections. The summary below represents an overview of the discussions held during the meeting.

The meeting was moderated by James Beardsley, Acting Director of the Cyber Security Directorate at the NRC. The presentation on industry lessons learned was given by William Gross of NEI, Michael Bailey of Duke Energy, and Jason Castro of TVA. It was followed by a presentation of NRC lessons learned, the status on the update of Regulatory Guide 5.71, and planned actions for upcoming Full Implementation cyber security inspections. The NRC presentation was given by Kim Lawson-Jenkins of the NRC Cyber Security Directorate. The presentations were followed by a moderated question and answer session. Questions were taken from attendees in the public meeting and from participants via the conference call and using the Go To Webinar application.

The first question asked the NRC why did the agency not wait to revise RG 5.71 since it will not affect the cybersecurity plans of currently operation nuclear power plants and those currently under construction. The NRC responded that the current version of RG 5.71 has been in place for more than 5 years. Updates will incorporate lessons learned during Milestones 1 – 7, recent table top exercises with industries, and industry guidance generated during the last 5 years. All of the information will be consolidated in RG 5.71.

A question was asked when would the insight gained from recent industry table top exercises and the Milestone 1-7 inspections be incorporated into industry guidance. The industry response was NEI 13-10 rev 5 should be updated by the end of 2016 to contain the outcomes of the table top exercises and workshops. SFAQs based on workshops should be completed in January-February 2017.

An industry representative noted that Slide 14 of NRC presentation mentioned the current threat environment. Has it changed? The NRC response was no, the current threat environment hasn't changed. However, any assessment should always review the threat environment.

An industry representative asked a question about Slide 7 of the NRC presentation regarding effectiveness of cyber security implementation. The example specifically noted several controls for an effective implementation of malware prevention. It was asked if alternate controls with justification would be acceptable for some facilities. The NRC responded yes; the material in the slide was listed only as an example and to highlight the intent of the individual security controls used in a specific implementation.

An individual asked what other government agencies apply 600 controls. The NRC replied that other government agencies must meet FISMA requirements. Department of Defense must implement tailored 800-53 controls and must implement additional controls (such as controls related to cryptography for high assurance systems).

An individual asked if the revision of Regulatory Guide 5.71 will include more information regarding what controls are applicable for components in industrial control systems such as PLCs. The NRC replied that yes, more information will be added in RG 5.71 on this item.

An individual asked if the NRC will endorse other standards on cybersecurity for nuclear security, such as international standards. The NRC responded that guidance will attempt to align with international standards but at this time there are no plans to endorse standards.

Three questions from an individual via the conference call –

1) Have utilities hired contractors to hack their systems. Industry response – no. Corporate IT performs analysis, scanning, penetration tests, table top exercises. Industry works with government agencies and shares information.
2) Has the NRC simulated attacks on nuclear power plants? No. The NRC has not performed activities such as the Force on Force exercises as are done for physical security. As mentioned during the presentation, the NRC has performed inspections for Milestones 1 – 7 and will begin full implementation inspections in 2017. Perhaps the NRC will perform simulated attacks in the future.
3) The third question was about response to a cyber incident. NRC mentioned again the new cyber reporting rule and guidance (NRC RG 5.83 and NEI 15.09) which details the interaction between industry and the NRC after a cyber attack. NRC also communicates with other government agencies such as DHS and the FBI.

A question was asked about dismissed employees. Industry responded that there is an immediate revocation of access when an unfavorable dismissal takes place. 10 CFR 73.56 discusses access authorization issues.

An individual asked how the NRC is addressing the zero-risk approach that was sometimes seen during Milestones 1-7 inspections? The NRC responded that full implementation training is taking place for all cyber inspectors. Also, NRC headquarter team members will participate in inspections and bring back lessons learned. The primary objective will be to have consistent implementation of inspections.

A question was asked about the synergy between fuel cycle work and inspection of operating nuclear plants. The NRC responded that information between the two groups is shared.

An individual asked about cyber inspector training in physical security. The NRC responded that the aforementioned full implementation training for cybersecurity inspectors included information about physical security (10 CFR 73.55).

A question again was asked about implementing NIST 800-53 controls for nuclear power plants. In addition to repeating the response given previously, the NRC noted the work done in NEI 13-10 and use of the graded approach to assist with effectively implementing the tailored NIST controls for nuclear power plants.

At the conclusion of the question and answer exchange, the open session of the public meeting ended. A brief closed session of the meeting was held between the NRC and industry. The NRC staff determined that the information to be discussed was Official Use Only – Security Related Information; therefore, the session of the meeting was closed to the public.