From: Andrew Brenner
To: Manny Sayoc; Clark Shurtleff
Cc: India Banks; Carolyn Lauron; Michelle Hayes
Subject: [External_Sender] RE: NRC Staff Feedback on 8/13 Cyber Security Public Meeting Materials
Date: Friday, August 9, 2024 11:49:38 AM
Attachments: (NP) Affidavit.pdf

Manny,

Apologies for not getting back to you yesterday. Please see our responses to the staff questions below. Please note that the questions themselves are not proprietary, however our responses to questions 5 and 6 are proprietary.

Please let me know if you have any questions.

Thanks,
Andrew

1. In several slides (ex. slides 4-7) regulation and guidance is cited. Clarify Holtec's plans, intent, and provide context why these are cited.

   Intent is to lay out our compliance plan. We intend to use RG 5.71 to comply with 10 CFR 73.54. RG 1.152 has requirements related to digital systems and cyber security and we intend to comply. Industry Guidance documents are references throughout the NRC guidance and we plan on referencing and using to help in complying per RG 5.71.
2. Where applicable, Holtec should identify what guidance they plan on using to meet requirements. For example, in slides 5 and 7, cybersecurity programs for commercial nuclear facilities can be met with RG 5.71 or NEI 08-09 (and accompanying guidance NEI 10-04 and 13-10). The staff would be able to provide better feedback if Holtec's plan was clarified.

   We plan to follow RG 5.71 and use the other guidance as input.
3. If it is Hotlec's intention to apply for an exemption from the cybersecurity requirements in 10 CFR 73.54, Holtec should explicitly state such. Holtec should engage with the NRC staff early, via pre-application meetings, if they intend to seek exemptions from the cybersecurity requirements.

   We currently have no plans to seek exemptions.
4. Many of the cited guidance are undergoing revisions and Holtec is advised that attending public meetings on those revisions may be beneficial (ex. guidance in slides 5, 7, and 9).

   Thank you for the feedback.
5. On SMR-300 Defensive Architecture, since this is a new design please clarify all acronyms, provide brief details regarding the functions (safety, security, and emergency preparedness) and interfaces of the systems, and indicate data communication boundary devices that separate security levels (slide 11).

   [[

●

●

●

●

●

●

●]]

6. Provide context for why the specific subset of SMR-300 Security Controls were selected (slide 12).

[[

.]]