U.S. Nuclear Regulatory Commission Summary of the January 31, 2023, Hybrid Public Meeting with NuScale Power, LLC to Discuss CFPP's Cybersecurity Program

Meeting Summary

The U.S. Nuclear Regulatory Commission (NRC) staff held a hybrid observation public meeting on January 31, 2023, with NuScale Power, LLC (NuScale), and Carbon Free Power Project, LLC (CFPP) to discuss NuScale's cybersecurity methodology and cybersecurity plan implementation approach for the CFPP combined license application (COLA.) This hybrid public meeting was a continuation of NRC staff's June 9, 2022, meeting with NuScale and CFPP on the same topic. The staff made the presentation slides for the open portion of the meeting available to the public prior to the meeting on NRC public meeting web page and via the Agency-wide Document Access and Management System (ADAMS)[1]. This hybrid public meeting took place at the NRC headquarters in Rockville, Maryland.

CFPP started the presentation by stating that CFPP's proposed approach to meet cybersecurity requirements in 10 CFR 73.54, "Protection of digital computer and communication systems and networks," were function-based. Specifically, the framework for CFPP's cybersecurity program was based on: (1) cybersecurity by design, i.e., defensive architecture and defense-in-depth; (2) National Institute of Standards and Technology (NIST) framework for critical infrastructure; (3) supply chain, and (4) cybersecurity for safety, security, and emergency planning (SSEP) functions. The NRC staff noted that while CFPP is allowed to use the NIST framework for determining the baseline security controls for all digital components, CFPP would need to map the resulting security controls to those in Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities" or NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors." Specifically, RG 5.71 and NEI 08-09 provide approaches that the NRC staff deems acceptable for complying with the requirements in 10 CFR 73.54 and are used by the NRC staff in support of their review per Section 13.6.6 (Cyber Security Plan) of NUREG-0800 (Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants). Therefore, such mapping would be necessary to facilitate the NRC staff review of CFPP's cybersecurity Plan. Furthermore, the NRC staff noted that there are several information resources available to NRC licensees such as NEI 10-04, "Identifying Systems and Assets Subject to the Cyber Security Rule," that CFPP should leverage as appropriate during the cybersecurity plan development. CFPP noted the NRC staff's feedback.

CFPP then described each element of its proposed cybersecurity approach. NuScale and CFPP summarized the open portion of the presentation by stating that CFPP is a completely digital controlled advanced reactor, and the protection of the digital infrastructure is required by both business and regulatory requirements. CFPP stated that NIST framework provides capability to use a risk-based maturity model cybersecurity program. Additionally, as determined by the application of the Electric Power Research Institute's (EPRI) technical assessment methodology (TAM), the SSEP components are further protected by additional controls. The NRC staff noted that the use of the EPRI TAM would warrant additional discussions as such methodology has not been used by previous NRC licensees as a means for justifying not implementing certain security controls. CFPP noted the NRC staff's feedback about the need to have future discussions on this topic.

[1] "Carbon Free Power Project (CFPP) Combined License Application (COLA) Presentation, Cybersecurity Program (Open Session)," PM-134195-NP, Rev. 0," (ML23023A130)

CFPP concluded its open portion of the presentation by stating that it intends to submit a White Paper on its cybersecurity methodology in March 2023 for the staff's review and feedback and will request additional public meetings to discuss the Cybersecurity White Paper.

At the conclusion of the open portion of the public meeting, the NRC staff opened the meeting to members of the public for questions and comments; however, there were no comments or questions from the public.

During the closed session, presenters from CFPP described CFPP's defensive architecture, plant operations platform, and CFPP's defense-in-depth in more technical detail. The NRC staff noted that architecture related topics such as the potential use of wireless technology and communication paths would warrant further discussions. CFPP noted the NRC staff's feedback.

At the conclusion of the closed portion of the meeting, the NRC staff asked several clarifying questions and requested CFPP to include adequate level of detail in its proposed White Paper that would enable the staff to have meaningful review and feedback.