

**NuScale Power - Comments and Review of**

Department of Homeland Security; Cybersecurity and Infrastructure Security Agency  
Secure Software Development Attestation Common Form (ICR 202311-1670-001)

Comment #	Section	Comments/Basis	Recommendation
1.	Page 2, 1 <sup>st</sup> & 2 <sup>nd</sup> paragraphs	For nuclear applications, document is incomplete because it invokes NIST SP 800-218 generally applicable for non-I&C, non-OT software, but does not include US NRC RG 1.152 Revision 3 for digital I&C / OT to which SMR vendors are committed.	Clarify – Regulatory Position C.2 in US NRC RG 1.152 Revision 3 governs secure development and operating environment for digital I&C / OT software, not NIST SP 800-218.
2.	Page 2, 4 <sup>th</sup> paragraph & items 1 through 3.	For nuclear applications, document does not clarify applicability: 1. To IT / non-I&C software? 2. To OT / digital I&C software? 3. To both? Note: this impacts response to comment 1 above.	Clarify – Digital I&C software is governed by RG 1.152 and RG 1.168 through RG-1.173, not NIST standards.
3.	Page 2, 4 <sup>th</sup> paragraph & items 1 through 3.	For nuclear applications, document is incomplete because it does not address the case of using commercial-off-the-shelf software for a safety-related activity.	Clarify – per US NRC RG 1.151, RG 1.168, and RIS 2016-05, EPRI TR-106439 governs dedication of commercial digital I&C / OT for a safety-related application, including its security parameters. NIST does not apply.  Per US NRC RG 1.231, EPRI TR-1025243 governs dedication of non-I&C / OT for a software-related application, including its security parameters. NIST does not apply.