PUBLIC SUBMISSION

SUNI Review Complete
Template=ADM-013
E-RIDS=ADM-03

ADD: Bridget Curran, Mekonen Bayssie, Mary Neely
Comment (5)
Publication Date: 3/3/2022
Citation: 87 FR 12208

As of: 5/4/22 10:02 AM
Received: May 02, 2022
Status: Pending_Post
Tracking No. l2p-dq2g-a5ej
Comments Due: May 02, 2022
Submission Type: Web

Docket: NRC-2021-0143
Cyber Security Programs for Nuclear Power Reactors

Comment On: NRC-2021-0143-0001
Cyber Security Programs for Nuclear Power Reactors

Document: NRC-2021-0143-DRAFT-0007
Comment on FR Doc # 2022-04464

Submitter Information

Email: areeve@nuscalepower.com
Organization: NuScale Power LLC.

General Comment

NuScale Power, LLC Submittal of Comments on Draft Regulatory Guide DG-5061, “Cyber Security Programs for Nuclear Power Reactors,”
Docket ID NRC–2021–0143
See attached file

Attachments

LO-118205_DG-5061 R1 Cyber Security_signed

May 2, 2022 Docket No. NRC-2021-0143

Office of Administration
Mail Stop: TWFN-7-A60M
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
ATTN: Program Management,
Announcements, and Editing Staff

SUBJECT: NuScale Power, LLC Submittal of Comments on Draft Regulatory Guide DG-5061, "Cyber Security Programs for Nuclear Power Reactors," Docket ID NRC–2021–0143

REFERENCES:
1. "Cyber Security Programs for Nuclear Power Reactors," 87 Fed. Reg. 12208, Thursday March 3, 2022.
2. Draft Regulatory Guide DG-5061, "Cyber Security Programs for Nuclear Power Reactors,Revision 1," February 2022 (ML2195A329).

In a Federal Register Notice dated March 3, 2022 (Reference 1), the U.S. Nuclear Regulatory Commission (NRC) issued for public comment the document DG-5061 (Reference 2), requesting that comments be submitted no later than May 2, 2022.

The attachment to this letter provides comments of NuScale Power, LLC (NuScale) on DG-5061.

This letter makes no regulatory commitments and no revisions to any existing regulatory commitments.

If you have any questions, please contact Mark Shaver at 541-360-0630 or at mshaver@nuscalepower.com.

Sincerely,

Carrie Fosaaen
Director, Regulatory Affairs
NuScale Power, LLC

Attachment: "NuScale Power Comments, U.S. Nuclear Regulatory Commission Draft Regulatory Guide DG-5061: 'Cyber Security Programs for Nuclear Power Reactors, RG 5.71 Draft Rev 1'"

NuScale Power Comments U.S. Nuclear Regulatory Commission Draft Regulatory Guide DG-5061 Cybersecurity Programs for Nuclear Power Reactors, RG 5.71 Draft Rev 1			
Comment #	Section	Comments/Basis	Recommendation
1.	C.3.1.3, pg. 19	The phrase “directly or indirectly affect the reactivity of an NPP” is overly broad	Consider using the guidance in NEI 10-04 “Loss of electrical output or reactor shutdown within 15 minutes.” The broad guidance of “directly or indirectly affects reactivity” is not quantitative as even minor changes in secondary plant parameters (loss of a 5th or 6th point heater, etc.) while affecting reactivity have little or no impact on plant operation or on the electrical output of the plant. This broad definition has caused uncertainty and has lead to expansion of assets defined as CDAs beyond what is required to ensure safety, security, and emergency preparedness (SSEP) functions or protection of the Bulk Electrical Supply (BES). This should be applied wherever reactivity or transient are used throughout the document. This will align with the text on page 20 and the revision of NEI 10-04 referenced on page 20 should be issued by the time this document is issued.
2.	C.3.1.3, pg. 19	The word transient in “could result in an unplanned reactor shutdown or transient” is unquantified and the recommendation for “reactivity affect” in Comment 1 should be applied.	Quantify “transient” similarly to reactivity change in Comment 1, using guidance similar to that in NEI 10-04 “Loss of electrical output or reactor shutdown within 15 minutes “to prevent overly broad classification of assets that do not have an impact on SSEP functions or the BES.
3.	C 3.1.3, pg. 21	The phrase “However, such systems are still vulnerable to cyber attack originating from internal sources” does not include the risk from malicious software or firmware inserted via the supply chain.	Change wording to “However, such systems are still vulnerable to cyber attack originating from internal sources, or insertion from the supply chain.”

NuScale Power Comments U.S. Nuclear Regulatory Commission Draft Regulatory Guide DG-5061 Cybersecurity Programs for Nuclear Power Reactors, RG 5.71 Draft Rev 1			
Comment #	Section	Comments/Basis	Recommendation
4.	C 3.1.3, pg. 21	The phrase "In addition, because of the abundance of off-the-shelf devices and peripherals that support communications technology…" should include wireless and Internet of Things.	Change wording to "In addition, because of the abundance of off-the-shelf devices and peripherals that support communications technology including wireless and Internet of Things (IoT)...."
5.	Pg. 55	Add SIEM to the list of Acronyms as it is used in the document.	Add "SIEM" (Security incident and event monitor).
6.	A.3.1.3, pg. 62	Phrase "[Licensee/Applicant]'s CST identified and documented CDAs that have a direct, supporting, or indirect role in the proper functioning of CSs" is overly broad and includes digital equipment that may not support an SSEP function in a CS.	Change to "[Licensee/Applicant]'s CST identified and documented CDAs that have a direct, supporting, or indirect role in the proper functioning of a CSs SSEP function."
7.	A.3.1.6, pg. 64	The application of controls does not allow for a quantitative risk-based approach to control assignment.	This comment assumes NRC acceptance of EPRI TAM or similar assessment mechanism as a method of control assignment. This reflects current cyber security best practice vs application of controls regardless of effectiveness. Add a new bullet point: With respect to technical security controls, [Licensee/Applicant] used …the following for each CDA: • Apply an NRC-approved quantitative risk-based analysis of the CDA to apply the controls in Appendix B to RG 5.71 to CDAs, OR; • (New 1st bullet point) "implementing all of the security …"

NuScale Power Comments U.S. Nuclear Regulatory Commission Draft Regulatory Guide DG-5061 Cybersecurity Programs for Nuclear Power Reactors, RG 5.71 Draft Rev 1			
Comment #	Section	Comments/Basis	Recommendation
8.	A.4.1.3, pg. 67	Vulnerability scanning is of limited use in detecting attacks. Add real time monitoring to this section. This is supported by monitoring requirements throughout this revision of RG 5.71.	Change section title to (or add new section that performs the same function) "Vulnerability Assessments, Scans and Monitoring." Add "[Licensee/Applicant] Employs real time monitoring of all CSs network traffic events and logs in real-time to analyze for changes in network communications or identified characteristics of a cyber-attack and maintains a current library of attack profiles. Automated collection and analysis of network traffic, CDA events and logs by a SIEM to provide notification to licensee in real time of security events and provide for incident response and forensic analysis."
9.	A.4.2.4, pg. 70	The section does not address changes to the cyber risk environment.	Add bulletpoint: "changes to the risk environment as documented in reports, alerts and notices from the Critical Infrastructure Security Agency (CISA), CDA vendors or credible sources."
10.	B.1.1, pg. B-1	To follow current best practice, access control policy should establish a Zero Trust architecture where practicable per NIST SP 800-207. This will drive the security architecture to current best practice while decreasing burden for password management, portable device and media control.	Add as initial control element: "establishes a Zero Trust Architecture in CSs and CDAs to the extent practicable. For CSs and CDAs where Zero Trust is not achievable the policy will;"…
11.	B.1.17, pg.B-9	Missing section number "as articulated in RG 5.71; Section numbers should be listed wherever RG 5.71 is referenced for clarity.	Add section number: "…as articulated in RG 5.71, C.3.2" , employ throughout document for clarity.

NuScale Power Comments U.S. Nuclear Regulatory Commission Draft Regulatory Guide DG-5061 Cybersecurity Programs for Nuclear Power Reactors, RG 5.71 Draft Rev 1			
Comment #	Section	Comments/Basis	Recommendation
12.	B.3.1, pg. B-17	This control intent does not add information to the reader beyond the title.	Change control intent to read: “The intent of this control is to ensure the development, documentation, and deployment of policies and associated implementing procedures to address requirements of CDAs and communication protection controls that establish network segmentation and boundary protection and cryptographic rules.”
13.	B.3.2, pg. B-18	Add real-time CDA monitoring as alternate control.	Add following as alternate control: “Employ real-time CDA configuration monitoring and blocking of modifications using an active cyber security monitoring system.”
14.	B.3.3, pg. B-19	The control intent assumes the licensee uses the same security level numbering format as RG 5.71 :”… Levels 3 and 4 from all other levels.”	Add reference in RG: “…Levels 3 and 4 from all other levels as shown in RG 5.71 Figure 6.”
15.	B.3.4, pg. B-19	Last bullet does not specify real time DOS monitoring.	Add real-time monitoring to control language for last bullet: “employing monitoring tools to detect indicators of denial-of-service attacks against CDAs in real time.”

NuScale Power Comments U.S. Nuclear Regulatory Commission Draft Regulatory Guide DG-5061 Cybersecurity Programs for Nuclear Power Reactors, RG 5.71 Draft Rev 1			
Comment #	Section	Comments/Basis	Recommendation
16.	B.3.6, pg. B-20	Control element: “Employ cryptographic mechanisms to recognize changes to information during transmission and upon receipt, unless otherwise protected by alternate physical measures” does not reflect control system protocols and communications. Internal ICS communications are in general not encrypted and encryption decryption within control systems cannot be easily performed except in systems with advanced controllers. Either delete the control element or specify when practicable. If the control element is intended for non ICS internal data the control should specify this.	Change control element to read “Employ cryptographic mechanisms to recognize changes to information during transmission over insecure networks and upon receipt from insecure networks where practicable, unless otherwise protected by alternate physical measures.”
17.	B.3.7, pg.B-20	Confidentiality is in general not a protected characteristic of ICS systems beyond Identifiers and authenticators (first bullet control element) since ICS systems rarely contain PII this control should specify security data.	Reword Control Intent to read: “The intent of this control is to ensure that the confidentiality of security and personal identifying information data is maintained as the data is passed to or from CDAs.”

NuScale Power Comments U.S. Nuclear Regulatory Commission Draft Regulatory Guide DG-5061 Cybersecurity Programs for Nuclear Power Reactors, RG 5.71 Draft Rev 1			
Comment #	Section	Comments/Basis	Recommendation
18.	B.3.15, pg. B-23	ICS systems rarely use DNS data or Name Services; this control should specify that DNS services be removed or disabled except where required. External DNS requests should be rejected. See NIST SP 800-82 Rev 2.	Change Control Intent and control to specify only for systems that use DNS. Change Control Intent to "For CDAs that use domain name services, ensure implementation and control of DNS services. Disable or remove DNS services in CDAs that do not use name resolution." Change Control to add control elements: • Disable DNS services or remove where practicable in CDAs that do not use name services. DNS services where required are configured to reject DNS queries to external domains.
19.	B.3.21, pg. B-25	Remove control, except for safety systems (these are covered in other standards). Diversity is difficult to obtain and is rarely implemented for non-safety systems / CDAs, while decreasing common vulnerabilities the inherent difficulties of implementing diverse control systems within a system make this control impractical and addition of control system architectures can add attack surfaces and exploit sequences. Remove control.	Delete control.

NuScale Power Comments U.S. Nuclear Regulatory Commission Draft Regulatory Guide DG-5061 Cybersecurity Programs for Nuclear Power Reactors, RG 5.71 Draft Rev 1			
Comment #	Section	Comments/Basis	Recommendation
20.	B.4	This entire section does not use best practice in current cyber security. Add Zero Trust as a new control with the remainder of the controls in B.4 to be applied when a Zero Trust architecture cannot be achieved. New ICS upgrades and installations will often be able to select a Zero Trust architecture vastly increasing the security of the entire system, addition of this control will drive licensees to current best practice.	Add new B.4 control as first control B.4.1 and renumber the rest with the addition of B.4.x: "Where Zero Trust cannot be achieved…rest of control B.4.1 implement a Zero Trust architecture as described in NIST SP 800-207." If control is added, update references to include NIST SP 800-207.
21.	B.4.2, pg. B-25	Add passphrases to second control element.	Change second control element to read: "passphrases and passwords have length and complexity commensurate with the required security."
22.	B.4.3, pg. B-28	Change password change requirement to reflect current best practice of not changing non-compromised sufficient passwords. Change of passwords that have sufficient complexity and have not been compromised does not add security and increases burden.	Add the statement: "Passwords of insufficient complexity and lengths for required security due to operational or technical limitations are changed every [describe the periods for each class of system; for example, 30 days for workstations, 3 months for CDAs in the vital area], passwords should be updated whenever a valid threat indicates risk of compromise."
23.	B.4.2, pg. B-28	Insert new control element for passphrases.	New control element to read: "passphrases should contain four words separated by spaces or characters and are used in preference to passwords where practicable."

NuScale Power Comments U.S. Nuclear Regulatory Commission Draft Regulatory Guide DG-5061 Cybersecurity Programs for Nuclear Power Reactors, RG 5.71 Draft Rev 1			
Comment #	Section	Comments/Basis	Recommendation
24.	B.5.2, pg. B-32	This control is incomplete, as a host-based intrusion-detection system (HIDS) will only detect changes to the Host (Server or PC that it runs on). This control should be expanded to include Network Intrusion Detection (NIDS) and Security Incident and Event Monitoring (SIEM). These are standard components of a cyber-security monitoring system and allow for detection of anomalous network traffic and attacks that a server especially a compromised one will not detect or alert on.	Add separate control B.5.3 to describe proper SIEM setup to include monitoring of all network traffic via the NIDS with compensating physical controls. Where not possible renumber controls to reflect.
25.	B.5.4, pg.B-33	Control does not reflect current best practice. Add Zero Trust.	Add new control element to emplace Zero Trust on CDAs and CDs where feasible.
26.	C.1.2, pg.C-2	Control does not reflect current best practice. Establishment of Zero Trust provides for media protection and control.	Add new control element to emplace Zero Trust on CDAs and CDs where feasible.
27.	C.3.3, pg. C-6	Control does not provide for continuous monitoring. Continuous monitoring of network communications, logs and events will provide for additional protection (detect) against malicious software (and firmware / hardware).	Add, as first control element: “Maintains a continuous monitoring system for CS and CDAs that provides for real-time analysis.”

NuScale Power Comments U.S. Nuclear Regulatory Commission Draft Regulatory Guide DG-5061 Cybersecurity Programs for Nuclear Power Reactors, RG 5.71 Draft Rev 1			
Comment #	Section	Comments/Basis	Recommendation
28.	C.8, pg. C-22	Add forensics and evidence retention to control elements.	Add control element: “Containment and eradication efforts to the extent practicable preserve forensic evidence of the attack, including but not limited to; data in memory, changes to software and firmware and storage media and preserve network information to analyze the attack.”
29.	C.8.4, pg. C-26	Add forensics and evidence collection and handling.	Add control element: “Cyber security forensics and evidence retention - This includes knowledge of computer forensic and evidence gathering and retention, legal requirements for handling and transmission of evidence.”
30.	C.8.6, pg. C-27	Add reporting Cyber Security Incidents to CISA (this is now required by regulation).	Add control element for licensee to inform CISA of cyber security attacks as required and consistent with site security program.
31.	C.10.4, pg. C-36	Add gathering and handling of evidence.	Add gathering, retention and handling of evidence to first control element.
32.	C.11.3, pg. C-41	Quarterly audits of baseline configurations are impractical and would be highly resource intensive (the audit would likely not finish before the next quarter starts) recommend changing to semi-annually. While feasible for the larger CSs the control does not establish the scope of the audits.	Change audit frequency to semi-annually.
33.	C.12.2, pg. C-46	The changing landscape of threats to ICS systems increasingly shifts to supply chain attacks from sophisticated adversaries. Recommend a robust supply chain risk management plan as described in NIST SP 800-161.	Add as C12.2.1 “Establishes a Cyber Security Supply Chain Risk Management Program” as reflected in NIST SP 800-161.