CARBON FREE
POWER PROJECT
155 North 400 West, Suite 480
Salt Lake City, UT 84103

LO-147494

August 17, 2023 Docket No. 99902052

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
One White Flint North
11555 Rockville Pike
Rockville, MD 20852-2738

SUBJECT: NuScale Power, LLC Submittal on Behalf of CFPP LLC Carbon Free Power Project (CFPP) Combined License Application (COLA) White Paper Entitled "Cyber Security Methodology for the Carbon Free Power Project." WP-147684, Revision 0

REFERENCES:

1. LO-134199, NuScale Power, LLC Submittal on behalf of Carbon Free PowerProject, LLC Entitled, "Carbon Free Power Project (CFPP) Combined License Application (COLA) Presentation, Cyber Security Program (Open Session)," PM-134195-NP, Revision 0 (ML23023A130)
2. LO-134200, NuScale Power, LLC Submittal on behalf of Carbon Free PowerProject, LLC Entitled, "Carbon Free Power Project (CFPP) Combined License Application (COLA) Presentation, Cyber Security Program (Closed Session)," PM-134196-P, Revision 0 (ML23023A136)

During an observation public meeting on January 31, 2023, CFPP presented to the NRC staff an overview of the CFPP cyber security methodology and cyber security program implementation approach (References 1 and 2). During this meeting the staff indicated that this topic would best be addressed through the submission of a white paper.

The purpose of this letter is to submit the enclosed Cyber Security Methodology for the staff's review on behalf of CFPP. The paper describes the methodology and implementation approach being used by the CFPP to develop the cyber security program.

Enclosure 1 is the proprietary version of WP-147684. CFPP requests that the proprietary version be withheld from public disclosure in accordance with the requirements of 10 CFR § 2.390. The enclosed affidavit (Enclosure 3) supports this request. Enclosure 2 is the nonproprietary version of the document.

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

If you have any questions, please contact Susan Baughn at 541-452-7319 or at sbaughn@nuscalepower.com.

Sincerely,

John Volkoff

John Volkoff
Manager, Combined License Applications
NuScale Power, LLC
COLA Support on behalf of CFPP LLC

Distribution: Matthew Mitchell, NRC
Omid Tabatabai, NRC
Thomas Hayden, NRC

Enclosure 1: "Cyber Security Methodology for the Carbon Free Power Project," WP-147684-P, Revision 0, proprietary version
Enclosure 2: "Cyber Security Methodology for the Carbon Free Power Project," WP-147684-NP, Revision 0, nonproprietary version
Enclosure 3: Affidavit of Carrie Fosaaen, AF-147495

Enclosure 1:

“Cyber Security Methodology for the Carbon Free Power Project,” WP-147684-P, Revision 0, proprietary version

Enclosure 2:

“Cyber Security Methodology for the Carbon Free Power Project,” WP-147684-NP, Revision 0, nonproprietary version

Cyber Security Methodology for the Carbon Free Power Project

Executive Summary

This paper describes the proposed methodology for meeting cyber security requirements specified by 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks" (Reference 1), for the Carbon Free Power Project (CFPP), which uses the NuScale Power Plant (NPP) US460 standard design. This proposed methodology is used to develop a cyber security program that incorporates current cyber security methods and leverages inherent design features of the US460 standard design.

The proposed strategy for addressing cyber security requirements specified by 10 CFR 73.54 for the CFPP is to:

1) Credit design features of the US460 standard design for mitigating postulated cyber attacks up to and including the design basis threat.
2) Protect the digital data and components from cyber attack by adopting a defense-in-depth cyber security program.
3) Use procedures to secure digital plant systems and components from cyber threats and counterfeits in the supply chain.
4) Describe the NPP defensive architecture for protecting digital assets such as digital computers, communication systems, networks, and related components that have a safety, security, or emergency preparedness (SSEP) function.
5) Use the CFPP Physical Protection Program required under 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage" (Reference 2), to protect digital assets that have an SSEP function. The CFPP physical security systems and physical security plan (PSP) are currently being developed.
6) Establish a risk-based cyber security program for digital assets that complies with the National Institute of Standards and Technology (NIST) Cyber Security White Paper 04162018, "Framework for Improving Critical Infrastructure Cyber Security" (Reference 3). The framework provides a governance structure emphasizing defense-in-depth application of controls and processes using accepted standards.
7) Mitigate residual cyber risk for digital assets that have an SSEP function by applying controls based on the process specified in the Electric Power Research Institute (EPRI) Technical Report 3002012752, "Cyber Security Technical Assessment Methodology: Risk Informed Exploit Sequence Identification and Mitigation" (Reference 4).

Because there are few safety-related and balance of plant (BOP) components for the CFPP that have or support an SSEP function, the focus of nuclear cyber security is on physical security systems and components. Therefore, the CFPP is proposing that U.S. Nuclear Regulatory Commission (NRC) regulated cyber security program requirements for the US460 standard

design be incorporated in the PSP as a nuclear cyber security subcomponent. A plant-wide baseline cyber security configuration and real-time cyber security monitoring serve as a defensive layer to protect and detect a cyber attack, and limit the consequences of such an attack, thus ensuring the integrity of SSEP functions.

1.0 Introduction

1.1 Purpose

The purpose of this cyber security white paper is to describe proposed methods and practices for protecting the CFPP digital assets from cyber attack. The CFPP Cyber Security Program is designed to provide protection for digital assets that perform SSEP functions, including electrical output, that could have an effect on the bulk electrical system (BES); and to protect digital assets that are relied upon for operating the CFPP in an efficient and economical manner. The proposed CFPP Cyber Security Program uses a risk-based maturity model that uses recognized standards for the protection of operational technology (OT) and meets the NRC cyber security requirements.

1.2 Abbreviations and Acronyms

Table 1-1. List of abbreviations and acronyms

Abbreviation	Meaning
BES	bulk electrical system
BOP	balance of plant
CFPP	Carbon Free Power Project
CIP	Critical Infrastructure Protection
CSM	cyber security monitoring system
DCS	distributed control system
DHRS	decay heat removal system
DMZ	demilitarized zone
EP	emergency preparedness
EPRI	Electric Power Research Institute
FPGA	field programmable gate array
I&C	instrumentation and controls
IEC	International Electrotechnical Commission
IT	information technology
LAN	local area network
MCR	main control room
MCS	module control system
MPS	module protection system
NEI	Nuclear Energy Institute
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NPM	NuScale Power Module

Table 1-1. List of abbreviations and acronyms (continued)

Abbreviation	Meaning
NPP	NuScale Power Plant
NRC	Nuclear Regulatory Commission
NSSS	nuclear steam supply system
OT	operational technology
PCS	plant control system
PN	plant network
PPS	plant protection system
PSP	physical security plan
SDIS	safety display and indication system
SSEP	safety, security, and emergency preparedness
TAM	Technical Assessment Methodology

2.0 Background

On October 26, 2006, the NRC published a proposed rulemaking on power reactor security requirements (Reference 5) that would codify similar requirements specified by a series of orders issued by the NRC following the terrorist attacks on September 11, 2001. In addition to requirements specified by these orders, the proposed rule included cyber security requirements with several other new provisions to ensure adequate protection against the design basis threat. The proposed cyber security requirements were located in 10 CFR 73.55(m).

On March 27, 2009, the NRC published the approved version of the power reactor security rule (Reference 6) with an effective date of May 26, 2009. Instead of locating cyber security requirements in 10 CFR 73.55(m) as originally proposed, the approved rule placed them in a new stand-alone section, 10 CFR 73.54. The requirements are designed to provide high assurance that digital assets are adequately protected against cyber attacks up to and including the design basis threat established by 10 CFR 73.1, “Purpose and Scope” (Reference 7). Specifically, the rule requires digital computer and communication systems and networks associated with SSEP functions be protected from cyber attacks that

- adversely impact the integrity or confidentiality of data and software.
- deny access to systems, services, or data.
- provide an adverse impact to the operations of systems, networks, and associated equipment.

To ensure cyber security requirements are fully satisfied, 10 CFR 73.54 and conforming changes made to applicable NRC licensing requirements require new applications for an operating or combined license to include a cyber security plan. The cyber security plan provides a description of how the requirements specified in 10 CFR 73.54 are addressed. When 10 CFR 73.54 was initially issued, it did not extend to the BOP. In 2010, the NRC expanded the cyber security rule scope to cover the BOP in order to establish a single regulator for cyber security at nuclear power plants. The reliability of all plant equipment was not ensured because the NRC cyber security requirements did not extend to all equipment within a nuclear power plant. Consequently, the Federal Energy Regulatory Commission issued Order 706-B, “Mandatory Reliability Standards for Critical Infrastructure Protection” (Reference 8), to clarify that BOP systems and equipment within a nuclear power plant not included within the scope of 10 CFR 73.54 are subject to compliance with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standard as approved in Order 706, “Mandatory Reliability Standards for Critical Infrastructure Protection” (Reference 9).

Commission paper SECY-10-0153, “Cyber Security - Implementation of the Commission’s Determination of Systems and Equipment within the Scope of Title 10 of the Code of Federal Regulations Section 73.54” (Reference 10), identified structures, systems, and components in the BOP having a nexus to radiological health and safety capable of directly or indirectly affecting reactivity of a nuclear power plant as within the scope of important-to-safety functions described in the cyber security rule.

Guidance for addressing the cyber security requirements specified by 10 CFR 73.54 is provided by Nuclear Energy Institute (NEI) 08-09, “Cyber Security Plan for Nuclear Power Reactors” (Reference 11), and Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Facilities” (Reference 12). Both documents provide cyber security programmatic guidance, architecture, and controls the NRC staff has found acceptable for demonstrating compliance with 10 CFR 73.54.

Recent updates to NEI 10-04, “Identifying Systems and Assets Subject to the Cyber Security Rule” (Reference 13), and NEI 13-10, “Cyber Security Control Assessments” (Reference 14), refined the definition of BOP assets within the scope of the cyber security rule to those that, if compromised, could cause the complete loss of electrical output or reactor shutdown within 15 minutes, thus establishing alignment with the current NERC critical infrastructure protection guidance in this regard.

3.0 Design Attributes of the US460 Standard Design

3.1 Nuclear Steam Supply System

The nuclear steam supply system (NSSS) for the NPP consists of six small modular pressurized water reactors. Each NuScale Power Module (NPM) consists of a reactor core, two steam generator tube bundles, and a pressurizer contained within a single reactor vessel located within a steel containment vessel. This assembly and the attached decay heat removal system (DHRS) passive condensers and valves for the NSSS and support systems comprise a single NPM. The DHRS and reactor are located in a below-grade ultimate heat sink. This design eliminates the need for external piping to connect the steam generators and pressurizer to the reactor pressure vessel. Natural circulation provides reactor coolant system flow, thereby eliminating the need for reactor coolant pumps.

The DHRS passively removes decay heat following a plant trip when the normal energy conversion system is not available. Actuation of the DHRS is accomplished automatically by the module protection system (MPS), which is manually initiated from the main control room (MCR) or from a remote location. For physical security purposes, the MPS design does not allow remote isolation of safety-related systems and therefore, completion of protective actions is ensured. If MCR evacuation is required before DHRS actuation, manual actuation of DHRS may be accomplished locally at the MPS cabinets. Following actuation, DHRS operational parameters are monitored from the MCR or alternate locations in the plant. Details of the design and redundancy bases of the actuation systems, including system actuation setpoints, reliability, and diversity, are provided in Chapter 7 of the NuScale Standard Design Approval Application (Reference 15).

The emergency core cooling system passively removes decay heat when a containment isolation signal is received and pressure is reduced as a result of decay heat removal by the DHRS. Similar to the DHRS, emergency core cooling system actuation is accomplished automatically by the MPS, and the emergency core cooling system cannot be isolated remotely from the MCR.

Safety systems of the NPP are designed to operate in a fail-safe mode without alternating current power, operator action, or external sources of cooling water for at least 72 hours after a design-basis event.

The NPP consists of six NPMs with individual secondary systems, turbine generators, and electrical distribution systems. The control systems for the individual module systems (NSSS and secondary plant) in each plant are segmented to prevent cyber attacks from affecting more than one NPM.

3.2 Secure Architecture and Protective Features for Digital Assets

{{

}}2(a),(c)

{{

}}2(a),(c)

{{

}}2(a),(c)

{{

}}2(a),(c)

3.3 Emergency Preparedness Systems and Components

The US460 standard design provides a high level of safety with regard to core damage and large release frequencies. The NRC acknowledged this by approving the NuScale Topical Report authorizing reduced emergency planning zones for plume exposure and allowing a site boundary emergency planning zone (Reference 16).

The NPP communications systems required for emergency preparedness (EP) functions are designed to ensure redundant, diverse means are available to prevent a single cyber attack from disabling EP functions as required by NUREG-0694/FEMA-REP-1, “Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants” (Reference 17). Reference 13 states that digital components that have a diverse alternate to perform EP functions need not be classified as critical digital assets. The NPP digital assets required to meet Reference 17 requirements that cannot satisfy diversity requirements to perform their functions are scoped for inclusion in the SSEP category with additional controls as defined by analysis using the EPRI Technical Assessment Method (TAM) process. The remainder of the digital assets that have an EP function but meet the diversity requirements are included in and protected by the baseline Cyber Security Program.

The EP systems and components required by Reference 17 for facilities and radiation monitoring are assessed for diversity and those systems that do not meet the diversity requirements are scoped into the SSEP category. All other EP digital components that meet the diversity requirements are included in the baseline Cyber Security Program.

3.4 Security Systems and Components

The CFPP Physical Security Program performs the functions of detect, assess, delay, and communicate. As it is vital to ensure the security systems, structures, and components perform their functions at all times, the digital assets that perform these functions are assigned to the SSEP classification in the Cyber Security Program. The security system digital assets are assigned to Security Level 4 in the secure digital instrumentation and control (I&C) architecture. Each security digital asset is evaluated for residual risk using the TAM process to assign controls for lowering the cyber risk below the allowable risk threshold.

Security systems and components do not allow inbound communication from other systems or components. The security digital assets are monitored by a security network monitoring system. The security systems and security system monitoring are site-specific.

3.5 Balance of Plant Systems and Components

The NPP is analyzed based on NEI 10-04 guidance for systems to be included in the SSEP scope of the CFPP Cyber Security Program. With respect to BES stability, a loss of 77 MWe has little impact on the grid. Using segmentation and compartmentalization of the BOP control scheme prevents a single cyber attack from affecting multiple NPMs. The BOP systems and components are analyzed by the program for their function and those with BOP impact as defined in NEI 10-04 are scoped into the SSEP category of components and included in the CFPP nuclear Cyber Security Program. Specific site impacts from BOP digital components are analyzed for BES impact determined by local requirements for grid stability as determined by the NERC requirements for that installation. Cyber security for the BOP devices that do not meet the criteria of SSEP set in NEI 10-04 is performed by the baseline Cyber Security Program.

3.6 Support Systems for Safety, Security, and Emergency Preparedness Functions

Digital assets of the following support systems were considered for potential impact on SSEP functions:

- electrical power systems (primary or backup)
- heating, ventilation, and air conditioning systems
- fire protection systems
- secondary power for detection and assessment
- support systems and equipment required to maintain diversity and defense-in-depth for safety systems (diverse actuation system and diverse display systems that are credited)

The US460 standard design does not require alternating current or direct current power to shut down or maintain shutdown conditions and there are no safety-related or augmented quality heating, ventilation, and air conditioning systems. Compromising fire protection equipment cannot prevent passive safety systems from shutting down the reactor or from maintaining shutdown conditions. The system assessment planning process includes digital components with regulatory impacts that are not included in the SSEP functions as defined in NEI 10-04, but have regulatory or operational impact requiring analysis and documentation in the SSEP scope program.

4.0 Best Practices for Addressing Cyber Security Requirements

The CFPP Cyber Security Program draws from best practices described in current United States and international standards for cyber security.

4.1 National Institute of Standards and Technology Framework for Industrial Control Systems

Recognizing that the national and economic security of the United States depends on the reliable function of critical infrastructure, the President issued Executive Order 13636, “Improving Critical Infrastructure Cybersecurity” (Reference 18), in February 2013. The order directed NIST to work with stakeholders to develop a voluntary framework based on existing standards, guidelines, and practices for reducing cyber risks to critical infrastructure. The “Cyber Security Enhancement Act of 2014” (Reference 19), reinforced the actions prescribed by Executive Order 13636.

Reference 3 was created through collaboration between industry and government. The voluntary framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the framework helps owners and operators of critical infrastructure to manage cyber security-related risk.

The NIST Framework (Reference 3) focuses on using business drivers to guide cyber security activities and considering cyber security risks as part of the organization's risk management processes. The Framework consists of three parts: the Framework Core, the Implementation Tiers, and the Framework Profiles. The Framework Core is a set of cyber security activities, outcomes, and informative references common across sectors and critical infrastructures. Elements of the core provide detailed guidance for developing individual organizational profiles. Through use of Framework Profiles, the Framework helps an organization align and prioritize its cyber security activities with its business or mission requirements, risk tolerances, and resources. The Implementation Tiers provide a mechanism for organizations to view and understand the characteristics of their approach for managing cyber security risk, which help in prioritizing and achieving cyber security objectives.

The Framework provides defense-in-depth and can be applied to any cyber security architecture standard by mapping specific controls and programmatic features to the Framework Core Functions of identify, protect, detect, respond, and recover.

The Department of Homeland Security provides guidance for adapting the Framework to nuclear facilities in the Cybersecurity and Infrastructure Security Agency Interim Guidance 2020-508, "Nuclear Sector Cyber Security Framework Implementation Guidance" (Reference 20), providing mapping of Framework functions and categories to the architecture features and controls found in NEI 08-09.

4.2 Electrical Power Research Institute Technical Assessment Method

The TAM provides a risk-based quantitative approach to cyber security assessment that tailors administrative and engineering security controls to the actual risk of compromise through cyber attack. It is optimized by using the applicable regulatory requirements and compliance map template.

The TAM is an assessment methodology to provide a quantitative assessment of the digital components included in the SSEP scope defined in the cyber security component of the PSP.

The TAM is a four-step approach:

1) Attack surface characterization: This step analyzes the asset identifying points of vulnerability to attack (e.g., network connections, ports, installed software) for each type of asset.
2) Allocation of security control methods: This step allocates standard control methods tailored to the identified attack surfaces that yields a quantifiable residual set of vulnerabilities not adequately addressed by standard control methods.
3) Allocation of site-specific control methods: This step comprises an analysis, which yields the characteristics of the site installation, providing for the application of site-specific control methods. This is quantified to ensure residual risk is either eliminated or is at an acceptable level.
4) Mapping to security control requirements: This step provides a matrix of control requirements for the individual assets and groups to allow establishing cyber security protection requirements tailored to the actual risk.

The TAM analyzes exploit sequences (i.e., actual attack methods) for specific assets and groups to quantify the effectiveness of controls rather than assuming the efficacy of controls. It manages asset vulnerability by performing recalculation of risk based on new threats and vulnerabilities, and then evaluating the application of existing controls.

The output of the TAM is mapped to industry standards and regulatory accepted cyber security guidance. The mapping is done by applying a control library to specific security requirements. The chosen control map for CFPP is from NEI 08-09.

4.3 Security for Industrial Automation and Automation Systems

While the CFPP Cyber Security Program uses NEI 08-09 controls, the International Electrotechnical Commission (IEC) standards in IEC 62443, “Security for Industrial Automation and Automation Systems” (Reference 21), provide cyber security guidance for incident response and segmentation used to inform the baseline cyber security processes. Specifically, IEC 62443

- is a set of security standards for the secure development of industrial automation and control systems.
- provides a thorough and systematic set of cyber security recommendations for use in OT systems.
- is a risk-based cyber security architecture for OT with defined maturity and risk levels.
- provides for granularity in the design of control systems through the use of zones, which equate to security levels, determined by risk analysis and conduits that are communication paths between zones.
- provides for segmentation inside a zone by sub-zones and their associated conduits.
- provides a basis for certification by several international standards groups and provides a certification for suppliers that meet the requirements of this series of standards.

5.0 CFPP Cyber Security Program

{{

}}2(a)(c)

{{

}}2(a)(c)

{{

}}$^{2(a)(c)}$

{{

}}2(a)(c)

{{

}}2(a)(c)

{{

}}2(a)(c)

{{

}}2(a)(c)

{{

}}2(a)(c)

{{

}}$^{2(a),(c)}$

6.0 Summary

A modern critical infrastructure facility that is highly automated requires cyber security as a fundamental function in the design, operation, and maintenance of the site. The CFPP uses cyber security by design to limit attack surfaces for cyber threats. The threat landscape is constantly changing and evolving making defense-in-depth, including real-time system monitoring and response, essential components of a cyber security program. An entire site approach to cyber security using the identify, protect, detect, respond, and recover functions outlined in the NIST Framework ensures the site's digital assets and operation are protected, while the defensive architecture and cyber security section of the PSP provides the enhanced level of security for the SSEP functions performed by digital components.

The CFPP is designed such that a cyber attack alone cannot cause a radiological release that is adverse to public health and safety. The limited number of digital components that have an effect on SSEP functions are managed by the Cyber Security Program within the PSP. The entire site is protected by the baseline Cyber Security Program that protects the valuable digital assets, site operation, and safety of the staff, and provides for reliable operation to support the energy needs of the community.

7.0 References

1) *U.S. Code of Federal Regulations*, “Protection of Digital Computer and Communication Systems and Networks,” Section 73.54, Part 73, Title 10, “Energy,” (10 CFR 73.54).

2) *U.S. Code of Federal Regulations*, “Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage,” Section 73.55, Part 73, Title 10, “Energy,” (10 CFR 73.55).

3) National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cyber Security,” CSWP 04162018, Version 1.1, April 16, 2018.

4) Electrical Power Research Institute, “Cyber Security Technical Assessment Methodology: Risk Informed Exploit Sequence Identification and Mitigation,” EPRI #3002012752, Revision 1, Palo Alto, CA, November 30, 2018.

5) U.S. Nuclear Regulatory Commission, “Power Reactor Security Requirements; Proposed Rule,” *Federal Register*, Vol. 71, No. 207, October 26, 2006, pp. 62663-62874.

6) U.S. Nuclear Regulatory Commission, “Power Reactor Security Requirements; Final Rule,” *Federal Register*, Vol. 74, No. 58, March 27, 2009, pp. 13925-13993.

7) *U.S. Code of Federal Regulations*, 10 CFR 73.1, “Purpose and Scope,” Section 73.1, Part 73, Title 10, “Energy,” (10 CFR 73.1).

8) U.S. Federal Energy Regulatory Commission, “Mandatory Reliability Standards for Critical Infrastructure Protection,” Order 706-B, March, 2009.

9) U.S. Federal Energy Regulatory Commission, “Mandatory Reliability Standards for Critical Infrastructure Protection,” Order 706, January, 2008.

10) U.S. Nuclear Regulatory Commission, “Cyber Security – Implementation of the Commission’s Determination of Systems and Equipment within the Scope of Title 10 of the Code of Federal Regulations Section 73.54,” Commission Paper SECY-10-0153, November 10, 2010.

11) Nuclear Energy Institute, “Cyber Security Plan for Nuclear Power Reactors,” NEI 08-09, Revision 6, April 2010.

12) U.S. Nuclear Regulatory Commission, “Cyber Security Programs for Nuclear Facilities,” Regulatory Guide 5.71, Revision 1, February 2023.

13) Nuclear Energy Institute, “Identifying Systems and Assets Subject to the Cyber Security Rule,” NEI 10-04, Revision 3, May 2022.

14) Nuclear Energy Institute, “Cyber Security Control Assessments,” NEI 13-10, Revision 6, August 2017.

15) NuScale Power, LLC, Submittal of the NuScale Standard Design Approval Application, Revision 0, January 31, 2023 (ML22339A066), Portland, OR.

16) NuScale Power, LLC, “Methodology for Establishing the Technical Basis for Plume Exposure Emergency Planning Zones at NuScale Small Modular Reactor Plant Sites,” TR-0915-17772-P-A, Revision 3.

17) U.S. Nuclear Regulatory Commission and Federal Emergency Management Agency, "Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants," NUREG-0694/FEMA-REP-1, Revision 2, December 2019.

18) Presidential Executive Order, "Executive Order - Improving Critical Infrastructure Cybersecurity," Executive Order 13636, February 12, 2013.

19) "Cyber Security Enhancement Act of 2014," Public Law 113-274 (PL 113-274).

20) Cybersecurity and Infrastructure Security Agency Interim Guidance 2020-508, "Nuclear Sector Cyber Security Framework Implementation Guidance for U. S. Power Reactors," Department of Homeland Security, 2020.

21) International Electrotechnical Commission, "Security for Industrial Automation and Automation Systems," IEC 62443, Parts 1-4, February 2019.

22) *U.S. Code of Federal Regulations*, "Cyber Security Event Notification," Section 73.77, Part 73, Title 10, "Energy," (10 CFR 73.77).

23) National Institute of Standards and Technology, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations," Special Procedure 800-161, Revision 1, May 2022.

Enclosure 3:

Affidavit of Carrie Fosaaen, AF-147495

NuScale Power, LLC

AFFIDAVIT of Carrie Fosaaen

I, Carrie Fosaaen, state as follows:

(1) I am the Vice President of Regulatory Affairs of NuScale Power, LLC (NuScale), and as such, I have been specifically delegated the function of reviewing the information described in this Affidavit that NuScale seeks to have withheld from public disclosure, and am authorized to apply for its withholding on behalf of NuScale.

(2) I am knowledgeable of the criteria and procedures used by NuScale in designating information as a trade secret, privileged, or as confidential commercial or financial information. This request to withhold information from public disclosure is driven by one or more of the following:

(a) The information requested to be withheld reveals distinguishing aspects of a process (or component, structure, tool, method, etc.) whose use by NuScale competitors, without a license from NuScale, would constitute a competitive economic disadvantage to NuScale.

(b) The information requested to be withheld consists of supporting data, including test data, relative to a process (or component, structure, tool, method, etc.), and the application of the data secures a competitive economic advantage, as described more fully in paragraph 3 of this Affidavit.

(c) Use by a competitor of the information requested to be withheld would reduce the competitor's expenditure of resources, or improve its competitive position, in the design, manufacture, shipment, installation, assurance of quality, or licensing of a similar product.

(d) The information requested to be withheld reveals cost or price information, production capabilities, budget levels, or commercial strategies of NuScale.

(e) The information requested to be withheld consists of patentable ideas.

(3) Public disclosure of the information sought to be withheld is likely to cause substantial harm to NuScale's competitive position and foreclose or reduce the availability of profit-making opportunities. The accompanying white paper reveals distinguishing aspects about the cyber security methodology and implementation approach by which NuScale develops its cyber security program.

NuScale has performed significant research and evaluation to develop a basis for this methodology and implementation approach and has invested significant resources, including the expenditure of a considerable sum of money.

The precise financial value of the information is difficult to quantify, but it is a key element of the design basis for a NuScale plant and, therefore, has substantial value to NuScale.

If the information were disclosed to the public, NuScale's competitors would have access to the information without purchasing the right to use it or having been required to undertake a similar expenditure of resources. Such disclosure would constitute a misappropriation of NuScale's intellectual property, and would deprive NuScale of the opportunity to exercise its competitive advantage to seek an adequate return on its investment.

(4) The information sought to be withheld is in the enclosed white paper entitled "Cyber Security Methodology for Carbon Free Power Project." WP-147684, Revision 0. The enclosure contains the designation "Proprietary" at the bottom of each page containing proprietary information. The information considered by NuScale to be proprietary is identified within double braces, "{{ }}" in the document.

(5) The basis for proposing that the information be withheld is that NuScale treats the information as a trade secret, privileged, or as confidential commercial or financial information. NuScale relies upon the exemption from disclosure set forth in the Freedom of Information Act ("FOIA"), 5 USC § 552(b)(4), as well as exemptions applicable to the NRC under 10 CFR §§ 2.390(a)(4) and 9.17(a)(4).

(6) Pursuant to the provisions set forth in 10 CFR § 2.390(b)(4), the following is provided for consideration by the Commission in determining whether the information sought to be withheld from public disclosure should be withheld:

(a) The information sought to be withheld is owned and has been held in confidence by NuScale.

(b) The information is of a sort customarily held in confidence by NuScale and, to the best of my knowledge and belief, consistently has been held in confidence by NuScale. The procedure for approval of external release of such information typically requires review by the staff manager, project manager, chief technology officer or other equivalent authority, or the manager of the cognizant marketing function (or his delegate), for technical content, competitive effect, and determination of the accuracy of the proprietary designation. Disclosures outside NuScale are limited to regulatory bodies, customers and potential customers and their agents, suppliers, licensees, and others with a legitimate need for the information, and then only in accordance with appropriate regulatory provisions or contractual agreements to maintain confidentiality.

(c) The information is being transmitted to and received by the NRC in confidence.

(d) No public disclosure of the information has been made, and it is not available in public sources. All disclosures to third parties, including any required transmittals to NRC, have been made, or must be made, pursuant to regulatory provisions or contractual agreements that provide for maintenance of the information in confidence.

(e) Public disclosure of the information is likely to cause substantial harm to the competitive position of NuScale, taking into account the value of the information to NuScale, the amount of effort and money expended by NuScale in developing the information, and the difficulty others would have in acquiring or duplicating the information. The information sought to be withheld is part of NuScale's technology that provides NuScale with a competitive advantage over other firms in the industry. NuScale has invested significant human and financial capital in developing this technology and NuScale believes it would be difficult for others to duplicate the technology without access to the information sought to be withheld.

I declare under penalty of perjury that the foregoing is true and correct. Executed on August 17, 2023.

Carrie Fosaaen