

November 11, 2016

Docket: PROJ0769

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

SUBJECT: NuScale Power, LLC Supplemental Proposal to Provide Technical Data Requirements for Restricted, Proprietary Class 1 Information

REFERENCES: 1. NuScale Letter LO-0916-51158 from Thomas A. Bergman (NuScale) to the U.S. Nuclear Regulatory Commission Document Control Desk, "NuScale Power, LLC Proposal," dated September 6, 2016 (ML16250A857)

In Reference 1, NuScale proposed a means for NRC access to NuScale restricted, proprietary class 1 information in order to facilitate the staff's technical review of NuScale submittals. The purpose of the information provided in the attachment to this letter is to supplement Reference 1 and identify the information technology (IT) technical requirements for handling restricted, proprietary class 1 information resulting in an acceptable process between NuScale and NRC.

On November 9, 2016, NuScale held a teleconference with the NRC in which:

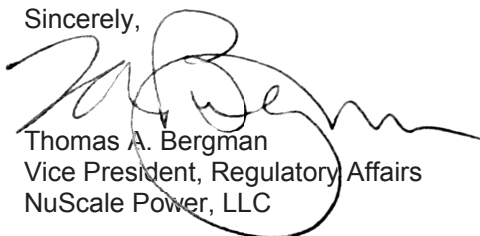
1. NuScale described its handling process and controls for restricted, proprietary class 1 information, and
2. The NRC Information Security Directorate (ISD) described the existing NRC IT processes in place to protect sensitive, proprietary information.

In the November 9 teleconference call, NRC and NuScale agreed that current NRC IT processes to protect sensitive, proprietary information could be used to protect NuScale restricted, proprietary class 1 information. In order to establish this process, NRC ISD staff requested that NuScale provide the IT technical requirements for handling, storage, in-use, transmission, receipt and conversion, and disposal of proprietary class 1 information. The attachment to this letter describes the NuScale IT data requirements.

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

Please feel free to contact Steve Mirsky at 240-833-3001 or at smirsky@nuscalepower.com if you have any questions.

Sincerely,



Thomas A. Bergman
Vice President, Regulatory Affairs
NuScale Power, LLC

Distribution: Frank Akstulewicz, NRC, TWFN-6C20
Greg Cranston, NRC, TWFN-6E55

Michael Mangefrida, NRC, TWFN-2C2
Anthony Markley, NRC, OWFN-12D20
Mark Tonacci, NRC, TWFN-6E55

Attachment: IT Data Requirements Handling, Storage, In-Use, Transmission, Receipt and Conversion,
and Disposal of NuScale Restricted, Proprietary Class 1 Information



General Handling Requirements

- Access shall be restricted to approved, need-to-know individuals with a current employment and/or contract status

Storage Requirements

- Printed Documents
 - Secure documents in a locked file cabinet or locked room when not in active use
 - Removal from restricted use area without authorization is prohibited
 - Copies of printed documents must be accounted for and tracked
- Electronic Documents
 - Must be stored in approved secure locations only
 - May not be transferred or stored on personally-owned devices
 - When not in active use, must be encrypted with FIPS 140-2 compliant technology using 2-factor authentication, one of which must be physical in nature. For example, CAC or PIV technology is acceptable.

In-Use Requirements

- Data that must be decrypted for use on a computing system must be placed on a computer without access to a public (Internet) or other intra-agency network. Typically, this is an air-gapped computer or network.
- Data that must be decrypted for use on a computing system must not be placed on any private/air-gapped network where it could be accessed by individuals without a need-to-know (i.e. by individuals working on an unrelated project)
- Data that must be decrypted for use on a computing system must either use whole-disk encryption and/or reside in a secured and locked facility. Removal from the facility without encryption must not be allowed.
- Decrypted data should ideally be decrypted only during active use, but must not be decrypted longer than is necessary for completion of the overall project work

Transmission Requirements

- Transmission of data over electronic means must be done with the same level of encryption and authentication protection as for storage.
- Transmission of printed data and documents over postal mail, or other courier services, must use sealed containers with tamper-evident seals and signature receipt acknowledgment.

Receipt and Conversion Requirements

- Data transmitted to the NRC by NuScale will be delivered using encryption and authentication technology
- Data may be converted to any NRC-preferred technology that complies with the storage requirements above

Disposal Requirements

- Printed documents and electronic media used for storage of encrypted data must be “destroyed” or “purged” according to NIST SP 800-88, Guidelines for Media Sanitation
- Printed documents and electronic media removed from secure area for purging or destruction must be in a locked container clearly intended for disposal