



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

January 6, 2011

Mr. Paul A. Harden
Site Vice President
FirstEnergy Nuclear Operating Company
Beaver Valley Power Station
Mail Stop A-BV-SEB1
P.O. Box 4, Route 168
Shippingport, PA 15077

SUBJECT: BEAVER VALLEY POWER STATION, UNIT NOS. 1 AND 2 - REQUEST FOR ADDITIONAL INFORMATION REGARDING THE REQUEST FOR APPROVAL OF THE CYBER SECURITY PLAN LICENSE AMENDMENT REQUEST (TAC NOS. ME4383 AND ME4384)

Dear Mr. Harden:

By letter dated July 22, 2010, FirstEnergy Nuclear Operating Company (the licensee) submitted a request to amend the Renewed Facility Operating Licenses for Beaver Valley Power Station, Unit Nos. 1 and 2 (BVPS-1 and 2). The licensee requested approval of the BVPS-1 and 2 Cyber Security Plan (CSP), provided a proposed CSP Implementation Schedule, and included a proposed revision to the Facility Operating License to incorporate the provisions for implementing and maintaining in effect the provisions of the approved CSP. The licensee's amendment request was based on a generic template developed by the Nuclear Energy Institute in concert with the industry.

The Nuclear Regulatory Commission (NRC) staff is reviewing the submittal and has determined that additional information is needed to complete its review. The specific questions are found in the enclosed request for additional information (RAI). The NRC staff is requesting a response to the RAI within 30 days of receipt.

The NRC staff considers that timely responses to RAIs help ensure sufficient time is available for NRC staff review and contribute toward the NRC goal of efficient and effective use of staff resources.

If you have any questions regarding this issue, please contact me at (301) 415-1016.

Sincerely,

A handwritten signature in black ink, appearing to read "Nadiyah S. Morgan", written over a horizontal line.

Nadiyah S. Morgan, Project Manager
Plant Licensing Branch I-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. 50-334 and 50-412

Enclosure:
RAI

cc w/encl: Distribution via Listserv

REQUEST FOR ADDITIONAL INFORMATION

REGARDING LICENSE AMENDMENT REQUEST FOR THE CYBER SECURITY PLAN

FIRSTENERGY NUCLEAR OPERATING COMPANY

BEAVER VALLEY POWER STATION, UNIT NOS. 1 AND 2

DOCKET NOS. 50-334 AND 50-412

By letter dated July 22, 2010 (Agencywide Documents Access and Management System Accession No. ML102080034), FirstEnergy Nuclear Operating Company (the licensee) submitted a license amendment request for the approval of the Beaver Valley Power Station, Unit Nos. 1 and 2 (BVPS-1 and 2) Cyber Security Plan (CSP). In order to complete the review, the Nuclear Regulatory Commission (NRC) staff needs the following additional information:

Section 3: Analyzing Digital Computer Systems And Networks

RAI 1 - Cyber Security Assessment Team Activities

Title 10 of the *Code of Federal Regulations* (10 CFR) Section 73.54(c)(1) states, "cyber security program must be designed to implement security controls to protect the assets identified by paragraph (b)(1) of this section from cyber attacks." The Nuclear Energy Institute (NEI) 08-09, Rev. 6, Section 3.1.2 states that a designated Cyber Security Assessment Team (CSAT) participate in the documentation of the required cyber security controls specified in Section 3.1.6; these include defense-in-depth strategies, technical, managerial, operational and, where necessary, alternative controls/countermeasures.

The BVPS-1 and 2 CSP, Section 3.1.2, states that the CSAT is charged with "reviewing and approving the required cyber security control application per Section 3.1.6 of this plan." The NEI 08-09, Rev. 6 guidance on Section 3.1.2 charges the CSAT with "documenting the required cyber security control application per Section 3.1.6 of this plan."

Explain how the controls referenced in Section 3.1.6 of the CSP will be documented, and which group or organization will be responsible for the documentation.

RAI 2 - Implementation of Alternative Security Controls or Countermeasures

10 CFR 73.54 (c)(1) indicates the "cyber security program must be designed to implement security controls to protect the assets identified by paragraph (b)(1) of this section from cyber attacks." The NEI 08-09, Rev. 6, Section 3.1.6, (2)(c) states that, when deploying alternative controls, the licensee will implement "alternative countermeasures that provide at least the same degree of cyber security protection as the corresponding cyber control;" (2)(d) states the licensee will implement "an alternative frequency or periodicity for the security control employed by documenting the basis for the alternate frequency or periodicity." In addition to (2)(a) and (2)(b), both (2)(c) and (2)(d), should be executed to ensure that selected alternative countermeasures effectively mitigate the absence of an established security control.

Enclosure

The BVPS-1 and 2 CSP states that the plant will implement (2)(a), (2)(b), and (2)(c) OR (2)(d) to ensure that selected alternative countermeasures effectively mitigate the absence of an established security control.

Clarify how the approach to either implement alternative controls that provide the same or greater degree of cyber security protections, or implement an alternative frequency or periodicity for the security control, provides the same or greater degree of protections for Critical Digital Assets.

Section 4: Establishing, Implementing, and Maintaining the Cyber Security Program

RAI 3 - Defense-in-Depth Protective Strategies – restrictive measures

Section 73.54(c)(2) of 10 CFR requires the licensee to apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks. Section 4.3, "Defense-in-Depth Protective Strategies," of the BVPS-1 and 2 CSP indicates that "communications initiated from lower levels to Critical Digital Assets at higher levels is: (1) eliminated, or (2) severely restricted, and cyber security controls and mitigation measures are in place that are analyzed, and described to demonstrate how the communications are severely restricted." The discussion does not elaborate on how these communications will be "severely restricted." Explain how communications from lower defensive levels to higher defensive levels will be "severely restricted."

Section Appendix B: Glossary

RAI 4 - Definition of Cyber Incident

Section 73.54(e)(2) of 10 CFR states, "the cyber security plan must include measures for incident response and recovery for cyber attacks." The definition of "incident" that the NRC finds acceptable and as stated in Regulatory Guide 5.71 is as follows: "Occurrence, caused by either human action or natural phenomena that may cause harm and that may require action." Furthermore, the NEI 08-09, Rev. 6, Appendix B (Glossary) guidance, defines cyber incident as "a digital-related adverse condition." Explain why the BVSP-1 and 2 CSP does not include a definition for "cyber incident."

January 6, 2011

Mr. Paul A. Harden
Site Vice President
FirstEnergy Nuclear Operating Company
Beaver Valley Power Station
Mail Stop A-BV-SEB1
P.O. Box 4, Route 168
Shippingport, PA 15077

SUBJECT: BEAVER VALLEY POWER STATION, UNIT NOS. 1 AND 2 - REQUEST FOR ADDITIONAL INFORMATION REGARDING THE REQUEST FOR APPROVAL OF THE CYBER SECURITY PLAN LICENSE AMENDMENT REQUEST (TAC NOS. ME4383 AND 4384)

Dear Mr. Harden:

By letter dated July 22, 2010, FirstEnergy Nuclear Operating Company (the licensee) submitted a request to amend the Renewed Facility Operating Licenses for Beaver Valley Power Station, Unit Nos. 1 and 2 (BVPS-1 and 2). The licensee requested approval of the BVPS-1 and 2 Cyber Security Plan (CSP), provided a proposed CSP Implementation Schedule, and included a proposed revision to the Facility Operating License to incorporate the provisions for implementing and maintaining in effect the provisions of the approved CSP. The licensee's amendment request was based on a generic template developed by the Nuclear Energy Institute in concert with the industry.

The Nuclear Regulatory Commission (NRC) staff is reviewing the submittal and has determined that additional information is needed to complete its review. The specific questions are found in the enclosed request for additional information (RAI). The NRC staff is requesting a response to the RAI within 30 days of receipt.

The NRC staff considers that timely responses to RAIs help ensure sufficient time is available for NRC staff review and contribute toward the NRC goal of efficient and effective use of staff resources.

If you have any questions regarding this issue, please contact me at (301) 415-1016.

Sincerely,

/RA/

Nadiyah S. Morgan, Project Manager
Plant Licensing Branch I-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. 50-334 and 50-412

Enclosure:
RAI

cc w/encl: Distribution via Listserv

DISTRIBUTION:

PUBLIC	RidsNrrLASLittle	RidsAcrsAcnw_MailCTR	LPLI-1 R/F
RidsNrrBeaverValley	RidsOGCRp	RidsNrrDorlDpr	CErlanger, NSIR
RidsRgn1MailCenter	RidsNrrDorlLplI-1	PPederson, NSIR	

ADAMS Accession No.: ML110050487

*See memo dated December 16, 2010

OFFICE	DORL/LPLI-1/PM	DORL/LPLI-1/LA	NSIR/DSP/BC	DORL/LPLI-1/BC
NAME	NMorgan	SLittle	CErlanger	NSalgado
DATE	1/6/11	1/6/11	12/16/2010*	1/6/11

OFFICIAL RECORD COPY