



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

March 7, 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 AMENDMENT APPLICATION FOR
APPROVAL OF THE CYBER SECURITY PLAN (TAC NOS. ME4383 AND
ME4384)

Dear Mr. Harden:

By letter dated July 22, 2010, as supplemented by letter dated February 3, 2011, 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.

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 "N. Morgan" followed by a flourish.

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), as supplemented my letter dated February 3, 2011 (ADAMS Accession No. ML110390066), 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:

RAI 1: Records Retention

Title 10 of the *Code of Federal Regulations* (10 CFR) Section 73.54(c)(2) requires licensees to design a cyber security program to ensure the capability to detect, respond to, and recover from cyber attacks. Furthermore, 10 CFR 73.54(e)(2)(i) requires licensees to maintain a Cyber Security Plan (CSP) that describes how the licensee will maintain the capability for timely detection and response to cyber attacks. The ability for a licensee to detect and respond to cyber attacks requires accurate and complete records and is further supported by 10 CFR 73.54(h), which states that the licensee shall retain all records and supporting technical documentation required to satisfy the requirements of 10 CFR 73.54 as a record until the Commission terminates the license for which the records were developed, and shall maintain superseded portions of these records for at least 3 years after the record is superseded, unless otherwise specified by the Commission.

The licensee's CSP in Section 4.13 states that Critical Digital Asset (CDA) audit records and audit data (e.g., operating system logs, network device logs) are retained for a period of time that is less than what is required by 10 CFR 73.54(h).

Explain the deviation from the 10 CFR 73.54(h) requirement to retain records and supporting technical documentation until the Commission terminates the license (or to maintain superseded portions of these records for at least 3 years) and how that meets the requirements of 10 CFR 73.54.

RAI 2: Implementation Schedule

The regulation at 10 CFR 73.54, "Protection of digital computer and communication systems and networks," requires licensees to submit a CSP that satisfies the requirements of this section for Commission review and approval. Furthermore, each submittal must include a proposed implementation schedule and the implementation of the licensee's cyber security program must be consistent with the approved schedule. 10 CFR 73.54(a) requires licensees to provide high assurance that digital computer and communication systems and networks are adequately

Enclosure

protected against cyber attacks, up to and including the design-basis threat (DBT). The completion of several key intermediate milestones (Items (a) through (g) below) would demonstrate progress toward meeting the requirements of 10 CFR 73.54. The Nuclear Regulatory Commission (NRC) staff's expectation is that the key intermediate milestones will be completed in a timely manner, but no later than December 31, 2012. The key CSP implementation milestones are as follows:

- (a) Establish, train and qualify Cyber Security Assessment Team, as described in Section 3.1.2, "Cyber Security Assessment Team," of the CSP.
- (b) Identify Critical Systems and CDAs, as described in Section 3.1.3, "Identification of Critical Digital Assets," of the CSP.
- (c) Implement cyber security defense-in-depth architecture by installation of deterministic one-way devices, as described in Section 4.3, "Defense-In-Depth Protective Strategies" of the CSP.
- (d) Implement the management, operational and technical cyber security controls that address attacks promulgated by use of portable media, portable devices, and portable equipment as described in Appendix D Section 1.19 "Access Control for Portable and Mobile Devices," of Nuclear Energy Institute (NEI) 08-09, Revision 6.
- (e) Implement observation and identification of obvious cyber related tampering to existing insider mitigation rounds as described in Appendix E Section 4.3, "Personnel Performing Maintenance and Testing Activities," and Appendix E Section 10.3, "Baseline Configuration" of NEI 08-09, Revision 6.
- (f) Identify, document, and implement cyber security controls to physical security target set CDAs in accordance with Section 3.1.6, "Mitigation of Vulnerabilities and Application of Cyber Security Controls," of the CSP.
- (g) Ongoing monitoring and assessment activities will commence for those target set CDAs whose security controls have been implemented, as described in Section 4.4, "Ongoing Monitoring and Assessment," of the CSP.
- (h) Full implementation of the CSP for all safety, security, and emergency preparedness functions.

Provide a revised CSP implementation schedule that identifies the appropriate milestones, completion dates, supporting rationale, and level of detail to allow the NRC to evaluate the licensee's proposed schedule and associated milestone dates which include the final completion date. It is the NRC's intention to develop a license condition incorporating your revised CSP implementation schedule containing the key milestone dates.

RAI 3: Scope of Systems

10 CFR 73.54(a) requires licensees to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the DBT as described in 10 CFR 73.1. In addition, 10 CFR 73.54(a)(1) states that the licensee shall protect digital computer and communication systems and networks associated with:

- (i) Safety-related and important-to-safety functions;
- (ii) Security functions;
- (iii) Emergency preparedness functions, including offsite communications; and
- (iv) Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

Subsequent to the issuance of the cyber security rule, the NRC stated that 10 CFR 73.54 should be interpreted to include structures, systems, and components (SSCs) in the balance of plant (BOP) that have a nexus to radiological health and safety (ADAMS Accession No. ML103490344, dated November 19, 2010). The SSCs in the BOP are those that could directly or indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient and are, therefore, within the scope of important-to-safety functions described in 10 CFR 73.54(a)(1). Furthermore, the NRC issued a letter to NEI dated January 5, 2011 (ADAMS Accession No. ML103550480) that provided licensees with additional guidance on one acceptable approach to comply with the Commission's policy determination.

Explain how the scoping of systems provided by licensee's CSP meets the requirements of 10 CFR 73.54 and the additional guidance provided by the NRC.

RAI 4: Definition of Cyber Incident

10 CFR Paragraph 73.54(c)(2) requires that "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, Revision 6, Appendix B (Glossary) guidance, defines cyber incident as "a digital-related adverse condition."

The BVPS-1 and 2 CSP do not contain a definition of "cyber incident." However, the BVPS-1 and 2 CSP makes 17 references to NEI 08-09, Appendix E (Operational and Management Controls), describing the CSP's implementation of the controls listed in that document. Section 4.6 of the BVPS-1 and 2 CSP lists six Incident Response topics that, it notes, are discussed in NEI 08-09, Appendix E. NEI 08-09, Appendix E discusses controls that describe an organization's responsibilities for addressing cyber incidents (e.g., Section 7, Attack Mitigation and Incident Response), and the detailed descriptions use various forms of the term "cyber incident." For example, the term "cyber security incident" or "cyber incident" is used in the following manner:

- Section 7.4 (Incident Handling), the control tasks the organization with “identification of what constitutes a cyber security incident;”
- Section 7.6 (Incident Response Assistance), the control states that the organization provides support personnel who offer advice and assistance to users “in response to and reporting of cyber security incidents;”
- Section 9.2 (Awareness Training), the control states that the organization must establish, implement, and document “training to include practical exercises to simulate actual cyber incidents.”

Because the CSP references controls that use the term “cyber incidents,” in the areas of training, attack mitigation, incident response and recovery, and audit generation, as well as establishing a Computer Security Incident Response Team, it is clear that “cyber incident” is an integral component of the BVPS-1 and 2 cyber security program. Please provide a definition of “cyber incident” such that the NRC staff can determine if the associated and contingent actions fully comply with 10 CFR 73.54.

March 7, 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.

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

Sincerely,
/ra/ (RGuzman for)
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	RidsAcrcAcnw_MailCTR	LPLI-1 R/F
RidsNrrBeaverValley	RidsOGCRp	RidsNrrDorIDpr	CErlanger, NSIR
RidsRgn1MailCenter	RidsNrrDorLpll-1	PPederson, NSIR	R. Pascarelli, NRR/DORL
T. Wengert, NRR/DORL	B. Singal, NRR/DORL		

ADAMS Accession No.: ML110630455 (*) Concurrence via e-mail (**) See memo dated March 4, 2011

OFFICE	DORL/LPLI-1/PM	DORL/LPLI-1/LA(*)	NSIR/DSP/BC (**)	DORL/LPLI-1/BC
NAME	RGuzman for NMorgan	SLittle	CErlanger	NSalgado
DATE	3/7/11	3/7/2011	3/4/2011	3/7/11

OFFICIAL RECORD COPY