



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

March 10, 2011

Mr. Mark B. Bezilla  
Site Vice President  
FirstEnergy Nuclear Operating Company  
Perry Nuclear Power Plant  
Mail Stop A-PY-A290  
P.O. Box 97, 10 Center Road  
Perry, OH 44081-0097

SUBJECT: PERRY NUCLEAR POWER PLANT, UNIT NO. 1 - REQUEST FOR  
ADDITIONAL INFORMATION RELATED TO THE LICENSE AMENDMENT  
REQUEST FOR APPROVAL OF THE PERRY CYBER SECURITY PLAN  
(TAC NO. ME4367)

Dear Mr. Bezilla:

By letter to the Nuclear Regulatory Commission (NRC) dated July 22, 2010 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML102100034), as supplemented by letters dated September 29, and November 29, 2010 (ADAMS Accession Nos. ML192899417 and ML103350211, respectively), and February 15, 2011 (ADAMS Accession No. ML110540414), FirstEnergy Nuclear Operating Company (FENOC or the licensee), submitted a license amendment request for approval of the Perry Nuclear Power Plant, Unit 1, Cyber Security Plan.

The NRC staff is reviewing your submittal and has determined that additional information is required to complete the review. The specific information requested is addressed in the enclosure to this letter. During a discussion with your staff on March 8, 2011, it was agreed that you would provide a response within 30 days from the date of this letter.

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

M. Bezilla

- 2 -

If circumstances result in the need to revise the requested response date, please contact me at (301) 415-3867.

Sincerely,

A handwritten signature in black ink, appearing to read "Michael Mahoney". The signature is written in a cursive style and is positioned above the typed name and title.

Michael Mahoney, Project Manager  
Plant Licensing Branch III-2  
Division of Operating Reactor Licensing  
Office of Nuclear Reactor Regulation

Docket No. 50-440

Enclosure:  
Request for Additional Information

cc w/encl: Distribution via Listserv

REQUEST FOR ADDITIONAL INFORMATION (RAI)

PERRY NUCLEAR POWER PLANT, UNIT NO. 1

DOCKET NO. 50-440

The Nuclear Regulatory Commission (NRC, the Commission) staff has reviewed the July 22, 2010 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML1021000334), as supplemented by letters dated September 29, and November 29, 2010 (ADAMS Accession Nos. ML192899417 and ML103350211, respectively), and February 15, 2011 (ADAMS Accession No. ML110540414), FirstEnergy Nuclear Operating Company submittal regarding the request for approval of the Perry Nuclear Power Plant (PNPP), Unit 1, Cyber Security Plan (CSP).

The NRC staff has determined that the following information is needed in order to complete its review:

**RAI No. 1: Records Retention**

Title 10 of the *Code of Federal Regulations* (10 CFR), Paragraph 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 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, 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 No. 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. Paragraph 73.54(a) of 10 CFR 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 design basis threat.

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 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 the 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 No. 3: Scope of Systems**

Paragraph 73.54(a) of 10 CFR 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 design basis threat 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 the Nuclear Energy Institute (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 PPNP's CSP meets the requirements of 10 CFR 73.54 and the additional guidance provided by the NRC.

#### **RAI No. 4: Definition of Cyber Incident**

Title 10 of the *Code of Federal Regulations* (10 CFR), Paragraph 73.54(e)(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 PNPP's CSP does not contain a definition of "cyber incident." However, PNPP's 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 PNPP's 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 PNPP’s CSP.

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.

M. Bezilla

- 2 -

If circumstances result in the need to revise the requested response date, please contact me at (301) 415-3867.

Sincerely,  
*/RA/*

Michael Mahoney, Project Manager  
Plant Licensing Branch III-2  
Division of Operating Reactor Licensing  
Office of Nuclear Reactor Regulation

Docket No. 50-440

Enclosure:  
Request for Additional Information

cc w/encl: Distribution via Listserv

**DISTRIBUTION:**

PUBLIC LPL3-2 R/F  
RidsNrrPMPerry Resource  
RidsAcrsAcnw\_MailCTR Resource  
RidsRgn3MailCenter Resource  
CErlanger, NSIR

RidsNrrDorlLpl3-2 Resource  
RidsNrrLATHarris Resource  
RidsOgcRp Resource  
RidsNrrDorlDpr Resource  
PPederson, NSIR

ADAMS Accession No. ML110670597

\*By Memo Dated

NRR-088

OFFICE	LPL3-2/PM	LPL3-2/LA	NSIR/DSP/ISCPB	LPL3-2/BC	LPL3-2/PM
NAME	MMahoney	SRohrer	CErlanger	RCarlson(NDiFrancisco for)	MMahoney
DATE	3/8/11	3/9/11	2/18/11 & 3/4/11*	3/10/11	3/10/11

OFFICIAL RECORD COPY