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

August 29, 2011

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

SUBJECT: PERRY NUCLEAR POWER PLANT, UNIT NO. 1 - ISSUANCE OF AMENDMENT RE: CYBER SECURITY PLAN (TAC NO. ME4367)

Dear Mr. Bezilla:

The U.S. Nuclear Regulatory Commission (NRC, the Commission) has issued the enclosed Amendment No. 158 to Facility Operating License (FOL) No. NPF-58 for the Perry Nuclear Power Plant, Unit No. 1 (PNPP). The amendment is in response to FirstEnergy Nuclear Operating Company's (FENOC's) application dated July 22, 2010, as supplemented by letters dated September 29, 2010, November 29, 2010, February 15, 2011, and April 8, 2011.

The amendment approves the Cyber Security Plan (CSP) and associated implementation schedule for PNPP. In addition, the amendment revises the existing license condition regarding physical protection in the PNPP FOL to require FENCO to fully implement and maintain in effect all provisions of the NRC approved CSP.

A copy of the Safety Evaluation is also enclosed. The Notice of Issuance will be included in the Commission's next biweekly *Federal Register* notice.

Sincerely,

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

Docket No. 50-440

Enclosures:
1. Amendment No. 158 to NPF-58
2. Safety Evaluation

cc w/encls: Distribution via Listserv

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

FIRSTENERGY NUCLEAR OPERATING COMPANY

FIRSTENERGY NUCLEAR GENERATION CORP.

OHIO EDISON COMPANY

DOCKET NO. 50-440

PERRY NUCLEAR POWER PLANT, UNIT NO. 1

AMENDMENT TO FACILITY OPERATING LICENSE

Amendment No. 158
License No. NPF-58

1. The U.S. Nuclear Regulatory Commission (the Commission) has found that:

   A. The application for license filed by FirstEnergy Nuclear Operating Company, et al., (the licensee, FENOC) dated July 22, 2010, as supplemented by letters dated September 29, 2010, November 29, 2010, February 15, 2011, and April 8, 2011, complies with the standards and requirements of the Atomic Energy Act of 1954, as amended (the Act), and the Commission's rules and regulations set forth in 10 CFR Chapter I;

   B. The facility will operate in conformity with the application, the provisions of the Act, and the rules and regulations of the Commission;

   C. There is reasonable assurance (i) that the activities authorized by this amendment can be conducted without endangering the health and safety of the public, and (ii) that such activities will be conducted in compliance with the Commission's regulations;

   D. The issuance of this amendment will not be inimical to the common defense and security or to the health and safety of the public; and

   E. The issuance of this amendment is in accordance with 10 CFR Part 51 of the Commission's regulations and all applicable requirements have been satisfied.

2. Accordingly, the Facility Operating License No. NPF-58 is hereby amended to add the following paragraph to license condition 2.E:

   FENOC shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The FENOC CSP was approved by License Amendment No. 158.

3. This license amendment is effective as of the date of its issuance. The implementation of the CSP, including the key intermediate milestone dates and the full implementation date, shall be in accordance with the implementation schedule submitted by the licensee on April 8, 2011, and approved by the U.S. Nuclear Regulatory Commission (NRC) staff with this license amendment. All subsequent changes to the NRC-approved CSP implementation schedule will require prior NRC approval pursuant to 10 CFR 50.90.

FOR THE NUCLEAR REGULATORY COMMISSION

Jacob I. Zimmerman, Chief
Plant Licensing Branch III-2
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Attachment: Changes to the Facility
Operating License

Date of Issuance: August 29, 2011

ATTACHMENT TO LICENSE AMENDMENT NO. 158

FACILITY OPERATING LICENSE NO. NPF-58

DOCKET NO. 50-440

Replace the following page of Facility Operating License (FOL) No. NPF-58 with the attached revised page. The revised page is identified by amendment number and contains marginal lines indicating the areas of change.

Remove	Insert
FOL No. NPF-58 Page 6	FOL No. NPF-58 Page 6

D. FENOC is exempted from: 1) the requirements of Section III.D.2(b)(ii), containment airlock testing requirements, Appendix J to 10 CFR Part 50, due to the special circumstance described in Section 6.2.6 of SER Supplement No. 7 authorized by 10 CFR 50.12(a)(2)(iii) and 2) the requirements of Section IV.F., Full Participation Exercise, of Appendix E to 10 CFR Part 50, due to the special circumstance described in the Exemption dated November 6, 1986. These exemptions are authorized by law, will not present an undue risk to the public health and safety, and are consistent with the common defense and security. The exemptions are hereby granted pursuant to 10 CFR 50.12. With the granting of these exemptions, the facility will operate, to the extent authorized herein, in conformity with the application, as amended, the provisions of the Act, and the rules and regulations of the Commission.

E. FENOC shall fully implement and maintain in effect all provisions of the Commission-approved physical security, training and qualification, and safeguards contingency plans, including amendments made pursuant to provisions of the Miscellaneous Amendments and Search Requirements revisions to 10 CFR 73.55 (61 FR 27817 and 27822) and to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The combined set of plans, which contain Safeguards Information protected under 10 CFR 73.21, is entitled: "Perry Nuclear Power Plant Physical Security Plan" Revision 2, submitted by letter dated May 18, 2006.

FENOC shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The FENOC CSP was approved by License Amendment No. 158.

F. Deleted

G. The licensees shall have and maintain financial protection of such type and in such amounts as the Commission shall require in accordance with Section 170 of the Atomic Energy Act of 1964, as amended, to cover public liability claims.

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

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION AND THE OFFICE OF NUCLEAR SECURITY AND INCIDENT RESPONSE RELATED TO AMENDMENT NO. 158 TO FACILITY OPERATING LICENSE NO. NPF-58 FIRSTENERGY NUCLEAR OPERATING COMPANY FIRSTENERGY NUCLEAR GENERATION CORP. OHIO EDISON COMPANY PERRY NUCLEAR POWER PLANT, UNIT NO. 1 DOCKET NO. 50-440

1.0 INTRODUCTION

By letter to the U.S. Nuclear Regulatory Commission (NRC, the Commission) dated July 22, 2010 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML102100034), as supplemented by letters dated September 29, 2010 (ADAMS Accession No. ML102800417), November 29, 2010 (ADAMS Accession No. ML103350211), February 15, 2011 (ADAMS Accession No. ML110540428), and April 8, 2011 (ADAMS Accession No. ML111030309), FirstEnergy Nuclear Operating Company (FENOC, the licensee) submitted a license amendment request (LAR). Included in that LAR was a request for approval of the licensee's Cyber Security Plan (CSP) and Implementation Schedule for the Perry Nuclear Power Plant (PNPP), Unit No. 1, as required by Section 73.54, "Protection of Digital Computer and Communication Systems and Networks," of Title 10 of the *Code of Federal Regulations* (10 CFR), and revision of Paragraph 2G of Facility Operating License (FOL) No. NPF-58 for PNPP. The proposed changes would require the licensee to fully implement and maintain in effect all provisions of the NRC-approved PNPP CSP.

On April 8, 2011, the licensee supplemented its CSP to address: (1) scope of systems in response to the October 21, 2010, Commission decision (Reference 1); (2) records retention; and (3) implementation schedule. The licensee submitted Revision 0 of the CSP incorporating all of the changes and/or additional information. Portions of the letters dated July 22, 2010, November 29, 2010, and April 8, 2011, and the entire letter dated February 15, 2011, contains sensitive unclassified non-safeguards information (security-related) and, accordingly, these portions are being withheld from public disclosure.

The supplements dated September 29, 2010, November 29, 2010, February 15, 2011, and April 8, 2011, provided additional information that clarified the application, and did not expand the scope of application as originally noticed, and did not change the NRC staff's initial proposed finding of no significant hazards consideration as published in the *Federal Register* on November 9, 2010 (75 FR 68834).

2.0 REGULATORY EVALUATION

2.1 General Requirements

Consistent with 10 CFR 73.54(a), the licensee must 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 (DBT), as described in 10 CFR 73.1. 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 (SSEP) functions. The rule specifies that digital computer and communication systems and networks associated with these functions must be protected from cyber attacks that would adversely impact the integrity or confidentiality of data and software; deny access to systems, services, or data; or provide an adverse impact to the operations of systems, networks, and associated equipment.

In the Staff Requirements Memorandum (SRM) COMWCO-10-0001, "Regulation of Cyber Security at Nuclear Power Plants," dated October 21, 2010 (Reference 1), the Commission stated that the NRC's cyber security rule at 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. The NRC staff determined that SSCs in the BOP that have a nexus to radiological health and safety are those that could directly or indirectly affect reactivity of a nuclear power plant (NPP), and are therefore within the scope of important-to-safety functions described in 10 CFR 73.54(a)(1).

2.2 Elements of a CSP

As stated in 10 CFR 73.54(e), the licensee must establish, implement, and maintain a CSP that satisfies the Cyber Security Program requirements of this regulation. In addition, the CSP must describe how the licensee will implement the requirements of the regulation and must account for the site-specific conditions that affect implementation. One method of complying with this regulation is to describe within the CSP how the licensee will achieve high assurance that all SSEP functions are protected from cyber attacks.

2.3 Regulatory Guide 5.71 and NEI 08-09, Revision 6

NRC Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities" (Reference 2), describes a regulatory position that promotes a defensive strategy consisting of a defensive architecture and a set of security controls based on standards provided in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," and NIST SP 800-82, "Guide to Industrial Control Systems Security," dated September 29, 2008. NIST SP 800-53 and NIST SP 800-82 are based on well-understood cyber threats, risks, and vulnerabilities, coupled with equally well-understood countermeasures and protective techniques. RG 5.71 divides the above-noted security controls into three broad categories: technical, operational, and management.

The RG 5.71 provides a framework to aid in the identification of those digital assets that licensees must protect from cyber attacks. These identified digital assets are referred to as "critical digital assets" (CDAs). Licensees should address the potential cyber security risks to CDAs by applying the defensive architecture and addressing the collection of security controls identified in RG 5.71. RG 5.71 includes a CSP template that provides one method for preparing an acceptable CSP.

The organization of RG 5.71 reflects the steps necessary to meet the requirements of 10 CFR 73.54. Section C.3 of RG 5.71 describes an acceptable method for implementing the security controls, as detailed in Appendix B, "Technical Controls," and Appendix C, "Operational and Management Controls." Section C.4 of RG 5.71 discusses the need to maintain the established Cyber Security Program, including comprehensive monitoring of the CDAs and the effectiveness of their security protection measures, ensuring that changes to the CDAs or the environment are controlled, coordinated, and periodically reviewed for continued protection from cyber attacks. Section C.5 of RG 5.71 provides licensees and applicants with guidance for retaining records associated with their cyber security programs. Appendix A to RG 5.71 provides a template for a generic cyber security plan which licensees may use to comply with the licensing requirements of 10 CFR 73.54. Appendices B and C provide an acceptable set of security controls, which are based on well-understood threats, vulnerabilities, and attacks, coupled with equally well-understood and vetted countermeasures and protective techniques.

The NEI 08-09, Revision 6, closely maps with RG 5.71; Appendix A of NEI 08-09, Revision 6, contains a CSP template that is comparable to Appendix A of RG 5.71. Appendix D of NEI 08-09, Revision 6, contains technical cyber security controls that are comparable to Appendix B of RG 5.71. Appendix E of NEI 08-09, Revision 6, contains operational and management cyber security controls that are comparable to Appendix C of RG 5.71.

In its letter to NEI dated May 5, 2010 (Reference 3), the NRC stated that the licensees may use the template in NEI 08-09, Revision 6 (Reference 4), to prepare an acceptable CSP, with the exception of the definition of "cyber attack." The NRC staff subsequently reviewed and approved by letter dated June 7, 2010 (Reference 5), a definition for "cyber attack" to be used in submissions based on NEI 08-09, Revision 6. The licensee submitted a CSP for the PNPP, Unit 1, that was based on the template provided in NEI 08-09, Revision 6, and included a definition of cyber attack acceptable to the NRC staff in the deviation table in Enclosure 3 of the CSP submitted by the licensee. Additionally, the licensee submitted a supplement to its CSP on February 15, 2011, to include information on SSCs in the BOP that, if compromised, could affect NPP reactivity.

The RG 5.71 and NEI 08-09, Revision 6, are comparable documents; both are based on essentially the same general approach and same set of technical, operational, and management security controls. The CSP submitted by the licensee was reviewed against the corresponding sections in RG 5.71.

3.0 TECHNICAL EVALUATION

The NRC staff performed a technical evaluation of the licensee's submittal. The licensee's submittal, with the exception of deviations described in Section 4.0 of this safety evaluation, generally conformed to the guidance in NEI 08-09, Revision 6, which was found to be acceptable by the NRC staff and comparable to RG 5.71 to satisfy the requirements contained

in 10 CFR 73.54. The staff reviewed the licensee's submittal against the requirements of 10 CFR 73.54 following the guidance contained in RG 5.71. The NRC staff evaluation of each section of the licensee's submittal is discussed below.

3.1 Scope and Purpose

The licensee's CSP establishes a means to achieve high assurance that digital computer and communication systems and networks associated with the following functions are adequately protected against cyber attacks up to and including the DBT:

- Safety-related and important-to-safety functions;
- Security functions;
- Emergency preparedness functions, including offsite communications; and
- Support systems and equipment which, if compromised, would adversely impact SSEP functions.

The licensee's CSP describes achievement of high assurance of adequate protection of systems associated with the above functions from cyber attacks by implementing and documenting:

- The baseline security controls as described in Appendix A, Section 3.1.6 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.3, described in RG 5.71; and
- A Cyber Security Program to maintain the established cyber security controls through a comprehensive life cycle approach as described in Appendix A, Section 4 of NEI 08-09, Revision 6, which is comparable to Appendix A, Section A.2.1, of RG 5.71.

Thus, the licensee's CSP, as originally submitted, is comparable to the CSP in NEI 08-09, Revision 6. However, in its submittal dated April 8, 2011, the licensee clarified its original submission and indicated that the scope of systems includes those BOP SSCs that have an impact on NPP reactivity if compromised. This is response to and consistent with SRM COMWCO-10-0001, in which the Commission stated that the NRC's cyber security rule provided in 10 CFR 73.54 should be interpreted to include SSCs in the BOP that have a nexus to radiological health and safety. The NRC staff determined that systems that have a nexus to radiological health and safety are those that could directly or indirectly affect reactivity of an NPP, and are therefore within the scope of important-to-safety functions described in 10 CFR 73.54(a)(1).

The NRC staff reviewed the CSP and the supplemental information submitted by the licensee and found no deviation from Regulatory Position C.3.3 in RG 5.71 and Appendix A, Section A.2.1 of RG 5.71. The NRC staff finds that the licensee established adequate measures to implement and document the Cyber Security Program, including baseline security controls.

Based on the above, the NRC staff finds that the PNPP CSP adequately establishes the Cyber Security Program, including baseline security controls.

3.2 Analyzing Digital Computer Systems and Networks and Applying Cyber Security Controls

The licensee's CSP states that the Cyber Security Program is established, implemented, and maintained as described in Section 3.1 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.1 described in RG 5.71 to:

- Analyze digital computer and communications systems and networks; and
- Identify those assets that must be protected against cyber attacks to satisfy 10 CFR 73.54(a).

The licensee's CSP describes how the cyber security controls in Appendices D and E of NEI 08-09, Revision 6, which are comparable to Appendices B and C in RG 5.71, are addressed to protect CDAs from cyber attacks. This section of the CSP submitted by the licensee is comparable to Regulatory Position C.3.1 in RG 5.71, without deviation.

Based on the above, the NRC staff finds that the CSP adequately addresses security controls.

3.3 Cyber Security Assessment and Authorization

The licensee provided information addressing the creation of a formal, documented, cyber security assessment and authorization policy. This included a description concerning the creation of a formal, documented procedure comparable to Section 3.1.1 of NEI 08-09, Revision 6.

The NRC staff finds that the licensee established adequate measures to define and address the purpose, scope, roles, responsibilities, management commitment, and coordination, and to facilitate the implementation of the cyber security assessment and authorization policy.

The NRC staff reviewed the above information and found no deviation from Section 3.1.1 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.1.1 and Appendix A, Section A.3.1.1, of RG 5.71.

Based on the above, the NRC staff finds that the CSP adequately established controls to develop, disseminate, and periodically update the cyber security assessment and authorization policy and implementing procedure.

3.4 Cyber Security Assessment Team (CSAT)

The CSAT responsibilities include conducting the cyber security assessment, documenting key findings during the assessment, and evaluating assumptions and conclusions about cyber security threats. The licensee's CSP outlines the requirements, roles and responsibilities of the CSAT comparable to Section 3.1.2 of NEI 08-09, Revision 6. It also describes that the CSAT has the authority to conduct an independent assessment.

The licensee's CSP describes that the CSAT will consist of individuals with knowledge about information and digital systems technology; NPP operations, engineering, and plant technical specifications; and physical security and emergency preparedness systems and programs. The CSAT description in the CSP is comparable to Regulatory Position C.3.1.2 in RG 5.71.

The licensee's CSP lists the roles and responsibilities for the CSAT which included performing and overseeing the cyber security assessment process; documenting key observations; evaluating information about cyber security threats and vulnerabilities; confirming information obtained during tabletop reviews, walk-downs, or electronic validation of CDAs; and identifying potential new cyber security controls.

The licensee's CSP noted in the ninth bullet in Section 3.1.2 that the CSAT would be involved in "reviewing and approving" cyber security controls; this is a deviation from the NEI 08-09, Revision 6, specification which states the CSAT would be responsible for "documenting" cyber security controls. The NRC staff requested clarification on how the controls would be documented. The licensee responded by stating that the documentation of controls would be ensured by a Cyber Security Specialist, but the preparation of the documentation could be accomplished by personnel from engineering, emergency preparedness, security or other disciplines, depending on the controls and the CDA under examination. The licensee submitted an updated CSP, and addressed the concern by inserting language in Section 3.1.6, "Mitigation and Vulnerabilities and Application of Cyber Security Controls," that "other plant organizations may be used to document the assessments. . ." The updated CSP notes in the same section that the CSAT would review and approve the usage of each cyber security control. This language supports the licensee's assertion that the documentation of security controls will occur and that the CSAT will have the ultimate responsibility for ensuring this occurs.

This section of the CSP submitted by the licensee is comparable to Regulatory Position C.3.1.2 in RG 5.71.

Based on the NRC staff's review of the CSP statement that cyber security controls will be documented by a Cyber Security Specialist and reviewed and approved by members of the CSAT, the NRC staff finds that the CSP adequately establishes the requirements, roles and responsibilities of the CSAT.

3.5 Identification of CDAs

The licensee's CSP states that the licensee will identify and document CDAs and critical systems, including a general description, the overall function, the overall consequences if a compromise were to occur, and the security functional requirements or specifications as described in Section 3.1.3 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.1.3 of RG 5.71.

Based on the above, the NRC staff finds that the CSP adequately describes the process to identify CDAs.

3.6 Examination of Cyber Security Practices

The licensee's CSP describes how the CSAT will examine and document the existing cyber security policies, procedures, and practices; existing cyber security controls; detailed

descriptions of network and communication architectures (or network/communication architecture drawings); information on security devices; and any other information that may be helpful during the cyber security assessment process as described in Section 3.1.4 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.1.2 of RG 5.71. The examinations will include an analysis of the effectiveness of the existing Cyber Security Program and cyber security controls. The CSAT will document the collected cyber security information and the results of their examination of the collected information. This section of the CSP submitted by the licensee is comparable to Regulatory Position C.3.1.2 in RG 5.71, without deviation.

Based on the above, the NRC staff finds that the CSP adequately describes the examination of cyber security practices.

3.7 Tabletop Reviews and Validation Testing

The licensee's CSP describes tabletop reviews and validation testing, which confirm the direct and indirect connectivity of each CDA and identify direct and indirect pathways to CDAs. The CSP states that validation testing will be performed electronically or by physical walkdowns. The licensee's plan for tabletop reviews and validation testing is comparable to Section 3.1.5 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.1.4 of RG 5.71.

Based on the above, the NRC staff finds that the CSP adequately describes tabletop reviews and validation testing.

3.8 Mitigation of Vulnerabilities and Application of Cyber Security Controls

The licensee's CSP describes the use of information collected during the cyber security assessment process (e.g., disposition of cyber security controls, defensive models, defensive strategy measures, site and corporate network architectures) to implement security controls in accordance with Section 3.1.6 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.3 and Appendix A.3.1.6 to RG 5.71. The CSP describes the process that will be applied in cases where security controls cannot be implemented.

The licensee's CSP states that before the licensee can implement security controls on a CDA, it will assess the potential for adverse impact in accordance with Section 3.1.6 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.3 of RG 5.71.

The licensee's CSP states that in the case of implementing alternative controls/ countermeasures that eliminate threat/attack vector(s) associated with one or more of the cyber security controls, that either an alternative countermeasure that provides at least the same degree of cyber security protection as the corresponding cyber security control will be implemented or an alternative frequency or periodicity for the security control will be implemented. The "or" condition in this statement is a deviation from NEI 08-09, Revision 6.

The NRC staff has reviewed this deviation and finds it to be acceptable on the basis that implementing alternative controls/countermeasures does not necessarily require an alternative frequency or periodicity be implemented.

Based on the NRC staff's review of CSP statement that the licensee will implement cyber security controls, implement alternative controls/countermeasures, or not implement a control as per Section 3.1.6 of the licensee's CSP, the NRC staff finds that this section of the CSP submitted by the licensee is comparable to Regulatory Position C.3.3 and Appendix A, Section A.3.1.6 or RG 5.71. The NRC staff also finds that this section of the CPS adequately describes mitigation of vulnerabilities and application of security controls.

3.9 Incorporating the Cyber Security Program into the Physical Protection Program

The licensee's CSP states that the Cyber Security Program will be reviewed as a component of the Physical Security Program in accordance with the requirements of 10 CFR 73.55(m). This is comparable to Section 4.1 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.4 of RG 5.71. This section of the CSP submitted by the licensee is comparable to Appendix A, Section A.3.2 in RG 5.71, without deviation.

Based on the above, the NRC staff finds that the CSP adequately describes review of the CSP as a component of the physical security program.

3.10 Cyber Security Controls

The licensee's CSP describes how the technical, operational and management cyber security controls contained in Appendices D and E of NEI 08-09, Revision 6, that are comparable to Appendices B and C in RG 5.71, are evaluated and dispositioned based on site-specific conditions during all phases of the Cyber Security Program. The CSP states that many security controls have actions that are required to be performed on specific frequencies and that the frequency of a security control is satisfied if the action is performed within 1.25 times the frequency specified in the control, as applied, and as measured from the previous performance of the action as described in Section 4.2 of NEI 08-09, Revision 6. This section of the CSP submitted by the licensee is comparable to Appendix A, Section A.3.1.6 in RG 5.71, without deviation.

Based on the above, the NRC staff finds that the CSP adequately describes implementation of cyber security controls.

3.11 Defense-in-Depth Protective Strategies

The submitted CSP describes the implementation of defensive strategies that ensure the capability to detect, respond to, and recover from a cyber attack. The CSP specifies that the defensive strategies consist of security controls, defense-in-depth measures, and the defensive architecture. The submitted CSP notes that the defensive architecture establishes the logical and physical boundaries to control the data transfer between these boundaries.
The licensee established defense-in-depth strategies by: implementing and documenting a defensive architecture as described in Section 4.3 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.2 in RG 5.71; a physical security program, including physical barriers; the operational and management controls described in Appendix E of NEI 08-09, Revision 6, which is comparable to Appendix C to RG 5.71; and the technical controls described in Appendix D of NEI 08-09, Revision 6, which is comparable to Appendix B to RG 5.71.

The NRC staff requested clarification from the licensee regarding which safety CDAs the licensee intended to locate outside of Level 4 and to provide justification for locating a safety CDA in Level 3. The licensee responded by letter dated February 1, 2011 (ADAMS Accession No. ML110390057), Attachment 1, and stated that FENOC would revise the CSP to state that safety CDAs are in Level 4. This is consistent with RG 5.71, Section C.7 of Appendix C, which states that CDAs that carry out safety functions should be allocated the highest degree of protection (i.e., Level 4); therefore, the NRC staff finds this clarification to be acceptable. This change was reflected in the revised CSP that was submitted on April 8, 2011 (ADAMS Accession No. ML111030065).

The licensee's CSP indicated that communications inherited from lower levels to CDAs at higher levels would be, "(1) eliminated or (2) severely restricted." Since the protection and isolating of CDAs at higher levels of security is vital to those defense-in-depth strategies at power plants, the NRC staff requested clarification from the licensee on how communications inherited from lower defense levels would be "severely restricted." The licensee responded by letter dated February 1, 2011 (ADAMS Accession No. ML110390057), Attachment 1, that FENOC would revise the CSP to indicate "communications from lower levels to CDAs at higher levels is eliminated." This is consistent with RG 5.71, Section C.7 of Appendix C, which states that initiation of communication from digital assets at lower security levels to digital assets at higher security levels is prohibited; therefore, the NRC staff finds this clarification to be acceptable. This change was reflected in the updated CSP that was submitted on April 8, 2011 (ADAMS Accession No. ML111030065).

The licensee's CSP indicated that "data flows from one level to other levels only through a device or devices that enforces documented cyber security policy between levels and detects, prevents, or delays that mitigates, and recovers from cyber attacks coming from lower cyber security levels." The NRC staff requested clarification about the specific sets of security controls that the licensee intended to implement to achieve this goal. The licensee responded by letter dated February 1, 2011 (ADAMS Accession No. ML110390057), Attachment 1, that FENOC would revise the CSP to remove the current site-specific description of the Defensive Architecture, including the phrase "data flows from one level to other levels only through a device or devices that enforces documented cyber security policy between levels and detects, prevents, or delays that mitigates, and recovers from cyber attacks coming from lower cyber security levels." The licensee revised the language to be identical with NEI 08-09, Revision 6, Section 4.3, Example 1, bullet 4. Therefore, the NRC staff finds this clarification to be acceptable. This change was reflected in the updated CSP that was submitted on April 8, 2011 (ADAMS Accession No. ML111030065).

The licensee's CSP indicated that "data transmission across defensive levels are analyzed, evaluated for risk, and protected." The NRC staff requested clarification from the licensee on the methodology for analyzing risk, and the security controls that will be enforced to achieve acceptable risk. In a letter dated February 1, 2011 (ADAMS Accession No. ML110390057), Attachment 1, the licensee responded that they would revise the CSP to remove the phrase, "data transmission across defensive levels are analyzed, evaluated for risk, and protected." The licensee subsequently submitted a revised CSP on April 8, 2011 (ADAMS Accession No. ML111030065) in which the defense-in-depth section was evaluated by NRC staff and found to be comparable to NEI 08-09, Revision 6, Section 4.3.

This section of the CSP submitted by the licensee is comparable to Regulatory Position C.3.2 and Appendix A, Section A.3.1.5 in RG 5.71.

Based on the licensee's comprehensive defense-in-depth protective strategies providing the capability to detect, respond to, and recover from a cyber attack, the NRC staff finds that the CSP adequately describes implementation of defense-in-depth protective strategies.

3.12 Ongoing Monitoring and Assessment

The licensee's CSP describes how ongoing monitoring of cyber security controls to support CDAs is implemented as described in Appendix E of NEI 08-09, Revision 6, which is comparable to Regulatory Positions C.4.1 and C.4.2 of RG 5.71. The ongoing monitoring program includes configuration management and change control; cyber security impact analysis of changes and changed environments; ongoing assessments of cyber security controls; effectiveness analysis (to monitor and confirm that the cyber security controls are implemented correctly, operating as intended, and achieving the desired outcome) and vulnerability scans to identify new vulnerabilities that could affect the security posture of CDAs. This section of the CSP submitted by the licensee is comparable to Regulatory Positions C.4.1 and C.4.2 of RG 5.71, without deviation.

Based on the above, the NRC staff finds that the CSP adequately describes ongoing monitoring and assessment.

3.13 Modification of Digital Assets

The licensee's CSP describes how cyber security controls are established, implemented, and maintained to protect CDAs. These security controls ensure that modifications to CDAs are evaluated before implementation that the cyber security performance objectives are maintained, and that acquired CDAs have cyber security requirements in place to achieve the site's Cyber Security Program objectives. This is comparable to Section 4.5 of NEI 08-09, Revision 6, which is comparable to Appendix A, Sections A.4.2.5 and A.4.2.6 of RG 5.71.

Based on the above, the NRC staff finds that the CSP adequately describes modification of digital assets.

3.14 Attack Mitigation and Incident Response

The licensee's CSP describes the process to ensure that SSEP functions are not adversely impacted due to cyber attacks in accordance with Section 4.6 of NEI 08-09, Revision 6, which is comparable to Appendix C, Section C.8 of RG 5.71. The CSP includes a discussion about creating incident response policy and procedures, and addresses training, testing and drills, incident handling, incident monitoring, and incident response assistance. It also describes identification, detection, response, containment, eradication, and recovery activities comparable to Section 4.6 of NEI 08-09, Revision 6. This section of the CSP submitted by the licensee is comparable to Appendix C, Section C.8 of RG 5.71, without deviation.

Based on the above, the NRC staff finds that the CSP adequately describes attack mitigation and incident response.

3.15 Cyber Security Contingency Plan

The licensee's CSP describes creation of a Cyber Security Contingency Plan and policy that protects CDAs from the adverse impacts of a cyber attack described in Section 4.7 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.3.2.7 and Appendix C, Section C.9 of RG 5.71. The licensee describes the Cyber Security Contingency Plan that would include the response to events. The plan includes procedures for operating CDAs in a contingency, roles and responsibilities of responders, processes and procedures for backup and storage of information, logical diagrams of network connectivity, current configuration information, and personnel lists for authorized access to CDAs. This section of the CSP submitted by the licensee is comparable to Regulatory Position C.3.3.2.7 of RG 5.71, without deviation.

Based on the above, the NRC staff finds that the CSP adequately describes the Cyber Security Contingency Plan.

3.16 Cyber Security Training and Awareness

The licensee's CSP describes a program that establishes the training requirements necessary for the licensee's personnel and contractors to perform their assigned duties and responsibilities in implementing the Cyber Security Program in accordance with Section 4.8 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.3.2.8 of RG 5.71.

The CSP states that individuals will be trained with a level of cyber security knowledge commensurate with their assigned responsibilities in order to provide high assurance that individuals are able to perform their job functions in accordance with Appendix E of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.3.2.8 of RG 5.71 and describes three levels of training: awareness training, technical training, and specialized cyber security training.

Based on the above, the NRC staff finds that the CSP adequately describes the cyber security training and awareness program.

3.17 Evaluate and Manage Cyber Risk

The licensee's CSP describes how cyber risk is evaluated and managed utilizing site programs and procedures comparable to Section 4.9 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.4 and Appendix C, Section C.13 of RG 5.71. The CSP describes the Threat and Vulnerability Management Program, Risk Mitigation, Operational Experience Program; and the Corrective Action Program and how each will be used to evaluate and manage risk. This section of the CSP submitted by the licensee is comparable to Regulatory Position C.4 and Appendix C, Section C.13 of RG 5.71, without deviation.

Based on the above, the NRC staff finds that the CSP adequately describes evaluation and management of cyber risk.

3.18 Policies and Implementing Procedures

The CSP describes development and implementation of policies and procedures to meet security control objectives in accordance with Section 4.10 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.5 and Appendix A, Section A.3.3 of RG 5.71. This includes the process to document, review, approve, issue, use, and revise policies and procedures.

The CSP also describes the licensee's procedures to establish specific responsibilities for positions described in Section 4.11 of NEI 08-09, Revision 6, which is comparable to Appendix C, Section C.10.10 of RG 5.71.

The licensee neglected to specify the title of the senior management official who is responsible for nuclear plant operations. Section 4.10 of NEI 08-09, Revision 6, offers the licensee several optional titles that can be selected, or the licensee can provide a senior management official in keeping with its organizational structure. The licensee does state that, "personnel responsible for the management and implementation of the program report to senior nuclear management." This omission does not impede the licensee's assurance that policies and procedures will be managed in a manner consistent with the requirements specified in Section 4.10 of NEI 08-09, Revision 6.

Based on the NRC staff's review of the licensees' statement in their CSP that the personnel responsible for the management and implementation of the cyber security program will report to senior nuclear management, the staff finds that the CSP adequately describes cyber security policies and implementing procedures.

3.19 Roles and Responsibilities

The licensee's CSP describes the roles and responsibilities for the qualified and experienced personnel, including the Cyber Security Program Sponsor, the Cyber Security Program Manager, Cyber Security Specialists, the Cyber Security Incident Response Team (CSIRT), and other positions as needed. The CSIRT initiates in accordance with the Incident Response Plan and initiates emergency action when required to safeguard CDAs from cyber security compromise and to assist with the eventual recovery of compromised systems. Implementing procedures establish roles and responsibilities for each of the cyber security roles in accordance with Section 4.11 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.1.2, Appendix A, Section A.3.1.2, and Appendix C, Section C.10.10 of RG 5.71.

The licensee's CSP contains deviations to the roles and responsibilities defined in the NEI 08-09, Revision 6, for the Cyber Security Program Manager and Cyber Security Specialist and creates a new role, Site Cyber Security Program Administrator. The roles and responsibilities deviations are as follows:

- The Cyber Security Program Manager is designated as the "corporate" Cyber Security Manager, and is identified with cyber security issues at the corporate or fleet-wide level. In addition to the responsibilities listed in the NEI 08-09, Revision 6, description, this position also interfaces with the newly created position, Site Cyber Security Program Administrator.

- The Site Cyber Security Program Administrator has several responsibilities that are associated with the NEI 08-09, Revision 6, description of the Cyber Security Specialist. The licensee's CSP states that the position can also be a Cyber Security Specialist, but the assigned duties indicate the person in this position will be a lead Cyber Security Specialist. The responsibilities are:

    - "Function as a single point of contact for issues related to cyber security"; this is formerly the responsibility of the Cyber Security Program Manager, but the distinction is made between the site/plant responsibilities of the Site manager and the corporate focus of the Cyber Security Program Manager.

    - "Initiates and coordinates the Cyber Security Incident Response Team (CSIRT) functions as required"; this is formerly the duty of the Cyber Security Program Manager as specified in NEI 08-09, Revision 6.

    - "Conduct cyber security audits, network scans, and penetration tests against CDAs as necessary"; this is formerly the duty of the Cyber Security Specialist as specified in NEI 08-09, Revision 6.

    - "Participates in the development and operation of the cyber security education, awareness, and training program"; this is a new responsibility not cited in the NEI 08-09, Revision 6, description for any position. The Site Cyber Security Program Administrator will be responsible for developing and operating programs that are approved by the Corporate Cyber Security Program Manager.

    - "Participates in the development and implementation of cyber security policies and procedures"; this is a new responsibility not cited in the NEI 08-09, Revision 6, description for any position. The Site Cyber Security Program Administrator will be responsible for developing and implementing cyber security policies and procedures that are approved by the Corporate Cyber Program Manager.

- In addition to the responsibilities that were transferred to the Site Cyber Security Program Administrator, as specified in NEI 08-09, Revision 6, an additional deviation was noted, whereby the licensee assigned the Cyber Security Specialist role the responsibility to:

    - "Ensure cyber security assessments of CDAs are performed and documented prior to being presented to CSAT for review and approval, this may include documenting the assessments or reviewing assessments provided by another organization such as Engineering, Emergency Preparedness, or Security, or a combination."

- The role of "Others" in NEI 08-09, Revision 6, refers to operators, engineers, technicians, and users who perform their assigned duties in accordance with the non-CSAT staff with the preparation of cyber security controls documentation, deviated from the NEI 08-09, Revision 6 text by inserting the phrase, "including

performing and documenting cyber security assessments of the CDAs, as requested by a Cyber Security Specialist." This deviation supports the licensee's approach, as discussed in Section 3.4, "Cyber Security Assessment Team," and Section 3.8, "Mitigation of Vulnerabilities and Application of Cyber Security Controls" of this safety evaluation.

While the licensee deviated from NEI 08-09, Revision 6, in Section 4.11 of its CSP, all of the specific roles and responsibilities have been designated to one of several cyber security personnel. Based on the licensee's CSP adequately addressing all of the roles and responsibilities, the NRC staff finds that the CSP adequately describes cyber security roles and responsibilities.

3.20 Cyber Security Program Review

The licensee's CSP describes how the Cyber Security Program establishes the necessary procedures to implement reviews of applicable program elements in accordance with Section 4.12 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.4.3 and Appendix A, Section A.4.3 of RG 5.71.

Based on the above, the NRC staff finds that the CSP adequately describes Cyber Security Program review.

3.21 Document Control and Records Retention and Handling

The licensee's CSP describes how the licensee has established the necessary measures and governing procedures to ensure that sufficient records of items and activities affecting cyber security are developed, reviewed, approved, issued, used, and revised to reflect completed work. The CSP states that superseded portions of certain records will be retained for at least three years after the record is superseded, while audit records will be retained for no less than 12 months in accordance with Section 4.13 of NEI 08-09, Revision 6. However, this guidance provided by industry to licensees did not fully comply with the requirements of 10 CFR 73.54.

In a letter dated February 28, 2011 (ADAMS Accession No. ML110600204), NEI sent to the NRC proposed language for licensees' use to respond to the generic records retention issue, to which the NRC had no technical objection and responded to NEI in a letter dated March 1, 2011 (ADAMS Accession No. ML110490337). The proposed language clarified the requirement by providing examples (without providing an all-inclusive list) of the records and supporting technical documentation that are needed to satisfy the requirements of 10 CFR 73.54. All records will be retained until the Commission terminates the license, and the licensee shall maintain superseded portions of these records for at least three years after the record is superseded, unless otherwise specified by the Commission.

By retaining accurate and complete records and technical documentation until the license is terminated, the inspectors, auditors, or assessors will have the ability to evaluate incidents, events, and other activities that are related to any of the cyber security elements described, referenced, and contained within the licensee's NRC-approved CSP. It will also allow the licensee to maintain the ability to detect and respond to cyber attacks in a timely manner, in the

case of an event. In a letter dated April 8, 2011, the licensee responded to the records retention issue using the language proposed by NEI in its letter dated February 28, 2011.

This section of the CSP submitted by the licensee is comparable to Regulatory Position C.5 and Appendix A, Section A.5 of RG 5.71, without deviation.

Based on the above, the NRC staff finds that the language the licensee proposes to adopt provides for adequate records retention and will support the licensee's ability to detect and respond to cyber attacks. The NRC staff further concludes that this section is comparable to Regulatory Position C.5 and Appendix A, Section A.5 of RG 5.71, without deviation.

Accordingly, the NRC staff finds that the CSP adequately describes cyber security document control and records retention and handling.

3.22 Implementation Schedule

The licensee's submitted CSP provides a proposed implementation schedule for the Cyber Security Program. In a letter dated February 28, 2011 (ADAMS Accession No. ML110600206), NEI sent to the NRC a template for licensees to use to submit their CSP implementation schedules, to which the NRC had no technical objection (Reference: Letter from NRC dated March 1, 2011, ADAMS Accession No. ML110070348). These key milestones include:

- Establish the CSAT;
- Identify CSs and CDAs;
- Install a deterministic one-way device between lower level devices and higher level devices;
- Implement the security control "Access Control For Portable And Mobile Devices";
- Implement observation and identification of obvious cyber related tampering to existing insider mitigation rounds by incorporating the appropriate elements;
- Identify, document, and implement cyber security controls as per "Mitigation of Vulnerabilities and Application of Cyber Security Controls" for CDAs that could adversely impact the design function of physical security target set equipment; and
- Commence ongoing monitoring and assessment activities for those target set CDAs whose security controls have been implemented.

In the letter dated April 8, 2011, the licensee provided a revised implementation schedule using the NEI template, with the exception of Milestone 6. The licensee revised Milestone 6 to address only the NEI 08-09, Revision 6, Appendix D, technical controls, excluding the operational and management controls, on the basis that implementing the technical controls for target set CDAs provides a high degree of protection against cyber-related attacks that could lead to radiological sabotage. Furthermore, the licensee explained that existing licensee

programs that are currently in place (e.g., physical protection, maintenance and work management, and configuration management, operational experience, etc.) provide a high degree of operational and management protection during the interim period until such time that the full Cyber Security Program is implemented.

3.23 Addition of License Condition

By letter dated July 22, 2010, the licensee proposed to add a paragraph to Paragraph 2.E of FOL No. NPF-58 for PNPP, to provide a license condition to require the licensee to fully implement and maintain in effect all provisions of the NRC-approved CSP. The NRC staff modified the proposed wording of the license condition described in the licensee's submittal dated July 22, 2010, and the licensee agreed with the revised license condition proposed by the NRC staff.

> FENOC shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The FENOC CSP was approved by License Amendment No. 158.

Based on the information in Section 3.0 of this safety evaluation and the modified license condition described above, the NRC staff concludes this is acceptable.

4.0 DIFFERENCES FROM NEI 08-09, REVISION 6

The NRC staff notes the following additional differences between the licensee's submission and NEI 08-09, Revision 6:

- In Section 3.1, "Scope and Purpose," the licensee clarified the definition of important-to-safety functions, consistent with SRM-COMWCO-10-0001.

- In Section 3.4, "Cyber Security Assessment Team (CSAT)," the licensee deviated by stating that cyber security controls will be documented by a Cyber Security Specialist and reviewed and approved by members of the CSAT.

- In Section 3.8, "Mitigation of Vulnerabilities and Application of Cyber Security Controls," the licensee deviated by stating in the case of implementing alternative controls/ countermeasures that eliminate threat/attack vector(s) associated with one or more of the cyber security controls, that either an alternative countermeasure that provides at least the same degree of cyber security protection as the corresponding cyber security control will be implemented or an alternative frequency or periodicity for the security control will be implemented.

- In Section 3.18, "Policies and Implementing Procedures," the licensee did not provide the title of the senior management official who is responsible for nuclear plant operations.

- In Section 3.19, "Roles and Responsibilities," the licensee deviated by assigning some of the specific roles and responsibilities to cyber security personnel in a manner that is different than NEI 08-09, Revision 6.

- In Section 3.21, "Document Control and Records Retention and Handling," the licensee clarified the definition of records and supporting documentation that will be retained to conform to the requirements of 10 CFR 73.54.

- In Section 3.22, "Implementation Schedule," the licensee submitted a revised implementation schedule, specifying the interim milestones and the final implementation date, including supporting rationale.

The NRC staff finds all of these deviations to be acceptable as discussed in the respective sections of this SE.

5.0 STATE CONSULTATION

In accordance with the Commission's regulations, the Ohio State official was notified of the proposed issuance of the amendment. The State official had no comments.

6.0 ENVIRONMENTAL CONSIDERATION

The amendment changes a requirement with respect to installation or use of a facility component located within the restricted area as defined in 10 CFR Part 20. The NRC staff has determined that the amendment involves no significant increase in the amounts, no significant change in the types of any effluents that may be released offsite, and that there is no significant increase in individual or cumulative occupational radiation exposure. The Commission has previously issued a proposed finding that the amendment involves no significant hazards consideration, and there has been no public comment on such finding published in the *Federal Register* on November 9, 2010 (75 FR 68834). Also, this amendment relates to safeguards matters and does not involve any significant construction impacts and relate to changes in recordkeeping, reporting, or administrative procedures or requirements. Accordingly, the amendment meets the eligibility criteria for categorical exclusion set forth in 10 CFR 51.22(c)(9), (10), and (12). Pursuant to 10 CFR 51.22(b), no environmental impact statement or environmental assessment need be prepared in connection with the issuance of the amendment.

7.0 CONCLUSION

The NRC staff's review and evaluation of the licensee's CSP was conducted using NRC staff positions established in the relevant sections of RG 5.71. Based on the NRC staff's review, the NRC finds that the licensee addressed the relevant information necessary to satisfy the requirements of 10 CFR 73.54, 10 CFR 73.55(a)(1), 10 CFR 73.55(b)(8), and 10 CFR 73.55(m), as applicable and that the licensee's Cyber Security Program provides high assurance that digital computer and communication systems and networks associated with the following are adequately protected against cyber attacks, up to and including the DBT as described in 10 CFR 73.1. This includes protecting digital computer and communication systems and networks associated with: safety-related and important-to-safety functions; security functions; emergency preparedness functions, including offsite communications; and support systems and equipment which, if compromised, would adversely impact SSEP functions.

Therefore, the NRC staff finds the information contained in this CSP to be acceptable and upon successful implementation of this program, operation of PNPP will not be inimical to the common defense and security.

The NRC staff has concluded, based on the considerations discussed above, that: (1) there is reasonable assurance that the health and safety of the public will not be endangered by operation in the proposed manner, (2) such activities will be conducted in compliance with the Commission's regulations, and (3) the issuance of this amendment will not be inimical to the common defense and security or to the health and safety of the public.

8.0 REFERENCES

1. Vietti-Cook, A. L., memorandum to R. W. Borchardt, U.S. Nuclear Regulatory Commission, "Staff Requirements - COMWCO-10-000 - Regulation of Cyber Security at Nuclear Power Plants," dated October 21, 2010 (ADAMS Accession No. ML102940009).

2. U.S. Nuclear Regulatory Commission, Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," dated January 2010 (ADAMS Accession No. ML090340159).

3. Correia, R., U.S. Nuclear Regulatory Commission, letter to Jack Roe, Nuclear Energy Institute, "Nuclear Energy Institute 08-09, 'Cyber Security Plan Template; Revision 6,'" dated May 5, 2010 (ADAMS Accession No. ML101190371).

4. Roe, J., Nuclear Energy Institute, letter to Scott Morris, U.S. Nuclear Regulatory Commission, "NEI 08-09, Revision 6, 'Cyber Security Plan for Nuclear Power Reactors; April 2010,'" dated April 28, 2010 (ADAMS Accession No. ML101180434).

5. Correia, R., U.S. Nuclear Regulatory Commission, letter to Christopher E. Earls, Nuclear Energy Institute, "Nuclear Energy Institute 08-09, 'Cyber Security Plan Template; Rev. 6,'" dated June 7, 2010 (ADAMS Accession No. ML101550052).

Principal Contributor: J. Green, NSIR

Date of issuance: August 29, 2011

August 29, 2011

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

SUBJECT: PERRY NUCLEAR POWER PLANT, UNIT NO. 1 - ISSUANCE OF AMENDMENT RE: CYBER SECURITY PLAN (TAC NO. ME4367)

Dear Mr. Bezilla:

The U.S. Nuclear Regulatory Commission (NRC, the Commission) has issued the enclosed Amendment No. 158 to Facility Operating License (FOL) No. NPF-58 for the Perry Nuclear Power Plant, Unit No. 1 (PNPP). The amendment is in response to FirstEnergy Nuclear Operating Company's (FENOC's) application dated July 22, 2010, as supplemented by letters dated September 29, 2010, November 29, 2010, February 15, 2011, and April 8, 2011.

The amendment approves the Cyber Security Plan (CSP) and associated implementation schedule for PNPP. In addition, the amendment revises the existing license condition regarding physical protection in the PNPP FOL to require FENCO to fully implement and maintain in effect all provisions of the NRC approved CSP.

A copy of the Safety Evaluation is also enclosed. The Notice of Issuance will be included in the Commission's next biweekly *Federal Register* notice.

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

Enclosures:
1. Amendment No. 158 to NPF-58
2. Safety Evaluation

cc w/encls: Distribution via Listserv
DISTRIBUTION:

PUBLIC	RidsNrrPMPerry Resource	LPL3-2 R/F
RidsOgcRp Resource	RidsNrrLASRohrer Resource	RidsNrrDorlLpl3-2 Resource
RidsRgn3MailCenter Resource	RidsNrrDorlDpr Resource	
RidsAcrsAcnw_MailCTR Resource	RidsNsirDsp Resource	

Amendment Accession No. ML111920382 * via e-mail

OFFICE	LPL3-2/PM	LPL3-2/LA	NSIR/DSP/ISCPB/BC	OGC(NLO w/comments)	LPL3-2/BC
NAME	MMahoney	SRohrer	CErlanger	BMizuno	JZimmerman
DATE	8/29/11	8/29/11	7/9/11*	8/16/11	8/29/11

OFFICIAL RECORD COPY