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

July 28, 2011

Vice President, Operations
Entergy Nuclear Operations, Inc.
Palisades Nuclear Plant
27780 Blue Star Memorial Highway
Covert, MI 49043-9530

SUBJECT: PALISADES NUCLEAR PLANT - ISSUANCE OF AMENDMENT REGARDING THE CYBER SECURITY PLAN: (TAC NO. ME4355)

Dear Sir :

The U.S. Nuclear Regulatory Commission has issued the enclosed Amendment No. 243 to Renewed Facility Operating License No. DPR-20 for Palisades Nuclear Plant. The amendment consists of changes to the Renewed Facility Operating License in response to your application dated July 26, 2010, supplemented by letters dated September 27, 2010, November 30, 2010, February 15, 2011, and April 4, 2011.

The amendment approves the cyber security plan (CSP) and associated implementation schedule, and revises Paragraph 2.E of Renewed Facility Operating License No. DPR-20 for Palisades Nuclear Plant, to provide a license condition to require the licensee to fully implement and maintain in effect all provisions of the NRC-approved CSP. The proposed change is generally consistent with Nuclear Energy Institute (NEI) 08-09, Revision 6, "Cyber Security Plan for Nuclear Power Reactors."

A copy of our related safety evaluation is also enclosed. The Notice of Issuance will be included in the Commission's biweekly *Federal Register* notice.

Sincerely,

Mahesh L. Chawla, Project Manager
Plant Licensing Branch III-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-255

Enclosures:
1. Amendment No. 243 to DPR-20
2. Safety Evaluation

cc w/encls: Distribution via ListServ

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

ENTERGY NUCLEAR OPERATIONS, INC.

DOCKET NO. 50-255

PALISADES NUCLEAR PLANT

AMENDMENT TO RENEWED FACILITY OPERATING LICENSE

Amendment No. 243
License No. DPR-20

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

   A. The application for amendment by Entergy Nuclear Operations, Inc. (the licensee), dated July 26, 2010, as supplemented by letters dated September 27, 2010, November 30, 2010, February 15, 2011, and April 4, 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;

   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 license is amended by changes as indicated in the attachment to the license amendment and Paragraph 2.C.(2) of Renewed Facility Operating License No. DPR-20 is hereby amended to read as follows:

   The Technical Specifications contained in Appendix A, as revised through Amendment No. 243, and the Environmental Protection Plan contained in Appendix B are hereby incorporated in the license. Entergy Nuclear Operations shall operate the facility in accordance with the Technical Specifications and the Environmental Protection Plan.

3. In addition, Paragraph 2.E of Renewed Facility Operating License No. DPR-20 is hereby amended with additional text to read as follows:

   ENO 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 Palisades CSP was approved by License Amendment No. 243.

4. This license amendment is effective as of the date of its issuance. The implementation of the cyber security plan (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 4, 2011, and approved by the 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

Timothy H. Betts For

Robert J. Pascarelli, Chief
Plant Licensing Branch III-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Attachment: Changes to the Renewed Facility Operating License

Date of Issuance: July 28, 2011

ATTACHMENT TO LICENSE AMENDMENT NO. 243

RENEWED FACILITY OPERATING LICENSE NO. DPR-20

DOCKET NO. 50-255

Replace the following page of the Renewed Facility Operating License No. DPR-20 with the attached revised page. The changed area is identified by a marginal line.

REMOVE	INSERT
Page 3	Page 3
Page 6	Page 6

(1) Pursuant to Section 104b of the Act, as amended, and 10 CFR Part 50, "Licensing of Production and Utilization Facilities," (a) ENP to possess and use, and (b) ENO to possess, use and operate, the facility as a utilization facility at the designated location in Van Buren County, Michigan, in accordance with the procedures and limitation set forth in this license;

(2) ENO, pursuant to the Act and 10 CFR Parts 40 and 70, to receive, possess, and use source and special nuclear material as reactor fuel, in accordance with the limitations for storage and amounts required for reactor operation, as described in the Updated Final Safety Analysis Report, as supplemented and amended;

(3) ENO, pursuant to the Act and 10 CFR Parts 30, 40, and 70, to receive, possess, and use byproduct, source, and special nuclear material as sealed sources for reactor startup, reactor instrumentation, radiation monitoring equipment calibration, and fission detectors in amounts as required;

(4) ENO, pursuant to the Act and 10 CFR Parts 30, 40, and 70, to receive, possess, and use in amounts as required any byproduct, source, or special nuclear material for sample analysis or instrument calibration, or associated with radioactive apparatus or components; and

(5) ENO, pursuant to the Act and 10 CFR Parts 30, 40, and 70, to possess, but not separate, such byproduct and special nuclear materials as may be produced by the operations of the facility.

C. This renewed operating license shall be deemed to contain and is subject to the conditions specified in the Commission's regulations in 10 CFR Chapter I and is subject to all applicable provisions of the Act; to the rules, regulations, and orders of the Commission now or hereafter in effect; and is subject to the additional conditions specified or incorporated below:

(1) ENO is authorized to operate the facility at steady-state reactor core power levels not in excess of 2565.4 Megawatts thermal (100 percent rated power) in accordance with the conditions specified herein.

(2) The Technical Specifications contained in Appendix A, as revised through Amendment No. 243, and the Environmental Protection Plan contained in Appendix B are hereby incorporated in the license. ENO shall operate the facility in accordance with the Technical Specifications and the Environmental Protection Plan.

(3) ENO shall implement and maintain in effect all provisions of the approved fire protection program as described in the Final Safety Analysis Report for the facility and as approved in the SERs dated 09/01/78, 03/19/80, 02/10/81, 05/26/83, 07/12/85, 01/29/86, 12/03/87, and 05/19/89 and subject to the following provisions:

D. The facility has been granted certain exemptions from the requirements of Section III, G of Appendix R to 10 CFR Part 50, "Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979." This section relates to fire protection features for ensuring the systems and associated circuits used to achieve and maintain safe shutdown are free of fire damage. These exemptions were granted in letters dated February 8, 1983, July 12, 1985, and July 23, 1985.

In addition, the facility has been granted certain exemptions from Appendix J to 10 CFR Part 50, "Primary Reactor Containment Leakage Testing for Water Cooled Power Reactors." This section contains leakage test requirements, schedules and acceptance criteria for tests of the leak-tight integrity of the primary reactor containment and systems and components which penetrate the containment. These exemptions were granted in a letter dated December 6, 1989.

These exemptions granted pursuant to 10 CFR 50.12, 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. With 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. ENO 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 (51 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 contains Safeguards Information protected under 10 CFR 73.21, is entitled: "Entergy Nuclear Palisades Nuclear Plant Physical Security Plan."

ENO 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 Palisades CSP was approved by License Amendment No. 243.

F. [deleted]

G. ENP and ENO 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 1954, as amended, to cover public liability claims.

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

SAFETY EVALUATION BY THE

OFFICE OF NUCLEAR SECURITY AND INCIDENT RESPONSE

RELATED TO AMENDMENT NO. 243 TO RENEWED

FACILITY OPERATING LICENSE NO. DPR-20

ENTERGY NUCLEAR OPERATIONS, INC.

PALISADES NUCLEAR PLANT

DOCKET NO. 50-255

1.0 INTRODUCTION

By letter dated July 26, 2010 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML102110090), supplemented by letters dated September 27, 2010, November 30, 2010, and April 4, 2011 (ADAMS Accession Nos. ML102710641, ML103340386, and ML110950688, respectively), Entergy Nuclear Operations (the licensee) submitted a license amendment request. Included in that license amendment was a request for approval of the licensee's Cyber Security Plan (CSP) and Implementation Schedule for the Palisades Nuclear Plant as required by Title 10 of the *Code of Federal Regulations* (10 CFR), Section 73.54 (Reference 1). The U.S. Nuclear Regulatory Commission (NRC, the Commission) staff provided the licensee requests for additional information (RAIs) regarding the staff's concerns with the CSP. By letter dated February 15, 2011 (ADAMS Accession No. ML110470452), the licensee submitted its response to these RAIs. Additionally, on April 4, 2011, the licensee supplemented their CSP (ADAMS Accession No. ML110950688), to address: 1) scope of systems in response to the October 21, 2010, Commission decision (Reference 5); 2) records retention; and 3) implementation schedule. The licensee submitted a Revision 0 of the CSP incorporating all of the changes and/or additional information as referenced in the RAI responses. Portions of letters dated July 26, 2010, September 27, 2010, February 15, 2011, and April 4, 2011, contain sensitive unclassified non-safeguards information (security-related) and, accordingly, those portions are withheld from public disclosure.

The supplemental letters dated September 27, 2010, November 30, 2010, February 15, 2011, and April 4, 2011, provided additional information that clarified the application, did not expand the scope of the application as originally noticed, and did not change the NRC staff's original proposed no significant hazards consideration determination as published in the Federal Register on December 7, 2010 (75 FR 76044).

Enclosure

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 October 21, 2010, Staff Requirements Memorandum (SRM)-COMWCO-10-0001 (Reference 5), 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 (RG) 5.71 and Nuclear Energy Institute (NEI) 08-09, Revision 6

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.

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 CSP 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.

The NRC staff stated in a letter (Subject: Nuclear Energy Institute [NEI] 08-09, "Cyber Security Plan Template, Revision 6)," dated May 5, 2010 (Reference 4), that the licensee may use the template in NEI 08-09, Revision 6 (Reference 3), 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 (ADAMS Accession No. ML101550052), a definition for "cyber attack" to be used in submissions based on NEI 08-09, Revision 6 . The licensee submitted a CSP for the Palisades Nuclear Plant 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 its letter to the NRC, dated July 26, 2010. In that letter, the licensee acknowledged it was using the definition of "cyber attack" that was approved by the NRC. Additionally, the licensee submitted a supplement to their CSP on April 4, 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 as both are based on essentially the same general approach and same set of technical, operational, and management security controls. The submitted CSP 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 exceptions of deviations described in Section 4.0, 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 NRC 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 their 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:

1. Safety-related and important-to-safety functions;

2. Security functions;

3. Emergency preparedness functions, including offsite communications; and

4. Support systems and equipment which, if compromised, would adversely impact SSEP functions.

The submitted 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 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

- Implementing and documenting a Cyber Security Program to maintain the established cyber security controls through a comprehensive life cycle approach as described in 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 4, 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 in response to and consistent with SRM-COMWCO-10-0001, "Regulation of Cyber Security at Nuclear Power Plants," October 21, 2010, in which the Commission stated that the NRC's cyber security rule at 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 those systems that have a nexus to radiological health and safety are those that could directly or indirectly affect reactivity of a NPP, and are therefore within the scope of important-to-safety functions described in 10 CFR 73.54(a)(1).

The licensee substituted "emergency planning" functions for "emergency preparedness" functions. Paragraph 73.54(a)(1) of 10 CFR requires that "The licensee shall protect digital computer and communication systems and networks associated with. . . (iii) emergency preparedness functions, and (iv) support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions." Section 73.54 of 10 CFR Part 70 does not address protection of digital assets, computers or communication systems that provide "emergency planning" functions. The NRC therefore submitted an RAI to the licensee, asking for clarification on the use of the term "emergency planning functions."

The licensee responded to the RAI by modifying the original statement in Section 2.1 (Scope and Purpose) of the CSP. The updated CSP correctly refers to the need to protect against cyber attack systems that perform "emergency preparedness functions." 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 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 submitted 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 submitted 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 submitted 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 submitted 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.

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 establishes the requirements, roles and responsibilities of the CSAT.

3.5 Identification of CDAs

The submitted CSP states that the licensee will identify and document CDAs and critical systems (CSs), 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.

This section of the CSP submitted by the licensee is comparable to Regulatory Position C.3.1.3 in RG 5.71, without deviation.

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 submitted 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 submitted 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.

This section of the CSP submitted by the licensee is comparable to Regulatory Position C.3.1.4 in RG 5.71, without deviation.

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 submitted 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 submitted CSP notes 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.

Based on the above, the NRC staff finds that the CSP adequately describes mitigation of vulnerabilities and application of security controls.

3.9 Incorporating the Cyber Security Program into the Physical Protection Program

The submitted 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 submitted 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 of RG 5.71; and the technical controls described in Appendix D of NEI 08-09, Revision 6, which is comparable to Appendix B of RG 5.71.

The CSP describes the defense-in-depth architecture as predicted on isolation of CDAs within

levels 2, 3, and 4. Furthermore, data flows from lower levels to high levels are described as being severely curtailed due to the implementation of appropriately configured firewalls, intrusion detection systems, air gaps, or deterministic one-way isolation devices such as data diodes or hardware virtual private networks (VPNs). The NRC staff's understanding of the hardware VPN is that it is a device that has security enhancement features, but is vulnerable to unauthorized intrusions in a like manner as traditional VPN software. Since the licensee proposed these devices as equally effective in isolating CDAs and CSs from cyber attack as other deterministic methods, the NRC staff submitted an RAI for further explanation on the characteristic, features and effectives of the hardware VPN. The licensee, in subsequent discussions with the NRC staff, indicated its intention to remove the hardware VPN as an option for isolating CDAs and CSs within levels 2, 3, and 4, from data flows initiated at lower levels. This change was implemented in the final version of the CSP submitted on April 4, 2011, and the NRC staff found it acceptable.

As noted in Section 3.1 above (Scope and Purpose), the licensee substituted "emergency plan functions" for "emergency preparedness functions" (as defined and noted in 10 CFR 73.54(a)(1)) in references to CDAs and CSs that would be protected via the submitted defense-in-depth architecture. On page 12 of the CSP, the licensee describes the implementation model for the defense-in-depth architecture, and characterizes the several types of CDAs that are protected within the proposed layers. The CSP notes in the third bullet that the "CDAs... that perform security or emergency plan functions..." and in the fourth bullet that the "CDAs... that perform or support Emergency Plan functions..." The NRC staff submitted a RAI for an explanation of the functions that are comprised under the term "Emergency Plan" and further requested that the licensee explain how the CDAs and CSs that perform "emergency preparedness" were protected under the submitted defense-in-depth architecture, as required by 10 CFR 73.54(a)(1). The licensee agreed to remove references to "emergency planning" and "emergency plan," and replace these terms with "emergency preparedness." This change was implemented in the final version of the CSP submitted on April 4, 2011, and the NRC staff found it acceptable.

On page 12 of the CSP, third bullet, the licensee characterized systems that were not required to be isolated at level 4, including those "... that perform safety monitoring, are within level 3." The term "safety monitoring" adequately describes functions typically performed by data acquisition systems. Accordingly, these systems are not required to be isolated at Level 4 and the NRC staff found this deviation to be acceptable.

With the above noted corrections and one acceptable deviation to the CSP, Section 4.3 of the CSP is comparable to Regulatory Position C.3.2 in RG 5.71.

Based on the above, the NRC staff finds that the CSP adequately describes implementation of defense-in-depth protective strategies.

3.12 Ongoing Monitoring and Assessment

The submitted CSP describes how ongoing monitoring of cyber security controls to support CDAs is implemented comparable to 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 submitted 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 Appendices A.4.2.5 and A.4.2.6 of RG 5.71.

This section of the CSP submitted by the licensee is comparable to Appendix A, Sections A.4.2.5 and A.4.2.6 of RG 5.71 without deviation.

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 submitted 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 submitted 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.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 submitted 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 (1) awareness training, (2) technical training, and (3) specialized cyber security training.

This section of the CSP submitted by the licensee is comparable to Regulatory Position C.3.3.2.8 of RG 5.71 without deviation.

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 submitted 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.

This section of the CSP submitted by the licensee is comparable to Regulatory Position C.3.5, Appendix A, Section A.3.3, and Appendix C, Section C.10.10 of RG 5.71, without deviation.

Based on the above, the NRC staff finds that the CSP adequately describes cyber security policies and implementing procedures.

3.19 Roles and Responsibilities

The submitted 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.

This section of the CSP submitted by the licensee 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, without deviation.

Based on the above, the NRC staff finds that the CSP adequately describes cyber security roles and responsibilities.

3.20 Cyber Security Program Review

The submitted 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.
This section of the CSP submitted by the licensee is comparable to Regulatory Position C.4.3 and Appendix A, Section A.4.3 of RG 5.71, without deviation.

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 submitted CSP describes that 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 stated 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 and a generic RAI was issued.

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 RAI, to which the NRC had no technical objection (Reference: Letter from NRC 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, 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 4, 2011 (ADAMS Accession No. ML110950688), the licensee responded to the records retention RAI using the language proposed by NEI in its letter dated February 28, 2011.

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 finds 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 concludes that the licensee's CSP adequately describes cyber security document control and records retention and handling.

3.22 Implementation Schedule

The 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 a letter dated April 4, 2011 (ADAMS Accession No. ML110950688), the licensee provided a revised implementation schedule using the NEI template. The NRC staff considers this April 4, 2011, supplement the approved schedule as required by 10 CFR 73.54.

The NRC staff acknowledges that, in its April 4, 2011, submittal, the licensee proposed several CSP milestone implementation dates as regulatory commitments. The NRC staff does not regard the CSP milestone implementation dates as regulatory commitments that can be changed unilaterally by the licensee, particularly in light of the regulatory requirement at 10 CFR 73.54, that "[i]mplementation of the licensee's cyber security program must be consistent with the approved schedule." As the NRC staff explained in its letter to all operating reactor licensees dated May 9, 2011 (ADAMS Accession No. ML110980538), the implementation of the plan, including the key intermediate milestone dates and the full implementation date, shall be in accordance with the implementation schedule submitted by the licensee and approved by the NRC. All subsequent changes to the NRC-approved CSP implementation schedule will require prior NRC approval pursuant to 10 CFR 50.90.

Based on the provided schedule ensuring timely implementation of those protective measures that provide a higher degree of protection against radiological sabotage, the NRC staff finds the Cyber Security Program implementation schedule is satisfactory.

3.23 Revision to License Condition 2.E

By letters dated July 26, 2010, and April 4, 2011, the licensee proposed to add a paragraph to Paragraph 2.E of Renewed Facility Operating License No. DPR-20 for PNP, 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 submittals dated July 26, 2010, and April 4, 2011, and the licensee agreed with the revised license condition proposed by the NRC staff.
The following paragraph is added to Paragraph 2.E of Renewed Facility Operating License No. DPR-20 for PNP.

ENO 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 Palisades CSP was approved by License Amendment No. 243.

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

4.0 DIFFERENCES FROM NEI 08-09, REVISION 6

In addition to the table of deviations found in Enclosure 1 of the licensee's CSP, 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 3.1, "Scope and Purpose," the licensee presented a deviation from the term "emergency planning" for "emergency preparedness" in its discussion of CSs that address safety-related and important-to-safety functions, security functions, and emergency preparedness functions. This deviation prompted an RAI from the NRC staff to determine the nature and impact of the deviation. The licensee responded to the RAI, and the NRC staff finds that this deviation has been resolved and is acceptable, as discussed in Section 3.1.

- In Section 3.11 "Defense-in-Depth Protective Strategies"

    - The licensee presented a deviation to the standard deterministic methods for isolating high level (3 or 4) CDAs, with the specification of "hardware VPNs" for isolating CDAs. This deviation prompted an RAI from the NRC staff. The licensee responded to the RAI, and the NRC staff finds that this deviation has been resolved and is acceptable, as discussed in Section 3.11.

    - The licensee presented a deviation in the use of the term "emergency planning" or "emergency plan" instead of the term "emergency preparedness." This deviation prompted an RAI from the NRC staff. The licensee responded to the RAI, and the NRC staff finds that this deviation has been resolved and is acceptable, as discussed in Section 3.11.

    - The licensee presented a deviation in the use of the term "safety monitoring" and the NRC staff found its use acceptable as discussed in Section 3.11.

- 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.

5.0 SUMMARY

The NRC staff's review and evaluation of the licensee's CSP was conducted using the 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: (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 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 the Palisades Nuclear Plant will not be inimical to the common defense and security.

6.0 STATE CONSULTATION

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

7.0 ENVIRONMENTAL CONSIDERATION

The amendment changes a requirement with respect to the 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, and no significant change in the types, of any effluents that may be released offsite, and 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 December 7, 2010 (75 FR 76044). Also, this amendment relates to safeguards

matters and does not involve any significant construction impacts and relates 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.

8.0 CONCLUSION

The Commission 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 the amendment will not be inimical to the common defense and security or to the health and safety of the public.

9.0 REFERENCES

1. Section 73.54 of 10 CFR, "Protection of Digital Computer and Communication Systems and Networks," U.S. Nuclear Regulatory Commission, Washington, DC, March 27, 2009.

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

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

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

5. SRM-COMWCO-10-0001, "Regulation of Cyber Security at Nuclear Power Plants," October 21, 2010. (ADAMS Accession No. ML102940009)

Principal Contributor: Joseph Green, NSIR

Date of issuance: July 28, 2011

Vice President, Operations
Entergy Nuclear Operations
Palisades Nuclear Plant
27780 Blue Star Memorial Highway
Covert, MI 49043-9530

July 28, 2011

SUBJECT: PALISADES NUCLEAR PLANT - ISSUANCE OF AMENDMENT REGARDING CYBER SECUTIY PLAN: (TAC NO. ME4355)

Dear Sir :

The U.S. Nuclear Regulatory Commission has issued the enclosed Amendment No. 243 to Renewed Facility Operating License No. DPR-20 for Palisades Nuclear Plant. The amendment consists of changes to the Renewed Facility Operating License in response to your application dated July 26, 2010, supplemented by letters dated September 27, 2010, November 30, 2010, February 15, 2011, and April 4, 2011.

The amendment approves the cyber security plan (CSP) and associated implementation schedule, and revises Paragraph 2.E of Renewed Facility Operating License No. DPR-20 for Palisades Nuclear Plant, to provide a license condition to require the licensee to fully implement and maintain in effect all provisions of the NRC-approved CSP. The proposed change is generally consistent with Nuclear Energy Institute (NEI) 08-09, Revision 6, "Cyber Security Plan for Nuclear Power Reactors."

A copy of our related safety evaluation is also enclosed. The Notice of Issuance will be included in the Commission's biweekly *Federal Register* notice.

Sincerely,

/RA/
Mahesh L. Chawla, Project Manager
Plant Licensing Branch III-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-255
Enclosures:
1. Amendment No. 243 to DPR-20
2. Safety Evaluation
cc w/encls: Distribution via ListServ

DISTRIBUTION:
PUBLIC
LPL3-1 r/f
RidsNrrDirsltsb Resource
RidsNrrPMPalisades Resource
RidsOgcRp Resource
PPederson, NSIR/DSP/ISCPB
RidsAcrsAcnw_MailCTR Resource
RidsNrrDorlDpr Resource
RidsNrrDorlLpl3-1 Resource
RidsNrrLABTully Resource
RidsRgn3MailCenter Resource
RSpitzberg, NSIR/DSP/ISCPB

ADAMS Accession No. ML111801243 *SE memo dated 05/26/11 (ML11131A006) and e-mail dated 07/09/11

OFFICE	LPL3-1/PM	LPL3-1/LA	NSIR/DSP/ISCPB/BC	OGC */NLO w/comments*	LPL3-1/BC
NAME	MChawla	BTully */Rohrer*	CErlanger	BMizuno	RPascarelli */TBeltz for*
DATE	07/14/11	07/09/11	05/26/11 & 07/9/11*	07/22/11	07/28/11

OFFICIAL RECORD COPY