



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

August 19, 2011

Vice President, Operations  
Entergy Nuclear Operations, Inc.  
James A. FitzPatrick Nuclear Power Plant  
P.O. Box 110  
Lycoming, NY 13093

SUBJECT: JAMES A. FITZPATRICK NUCLEAR POWER PLANT - ISSUANCE OF  
AMENDMENT RE: LICENSE AMENDMENT REQUEST - CYBER SECURITY  
PLAN (TAC NO. ME4267)

Dear Sir or Madam:

The Commission has issued the enclosed Amendment No. 300 to Renewed Facility Operating License (FOL) No. DPR-59 for the James A. FitzPatrick Nuclear Power Plant (JAFNPP). The amendment is in response to your application dated July 15, 2010, as supplemented by letters dated February 15 and April 4, 2011.

The licensee's application for the amendment to the Renewed FOL includes: (1) the proposed JAFNPP Cyber Security Plan (CSP), (2) an implementation schedule, and (3) a proposed sentence to be added to the existing renewed FOL Physical Protection license condition for JAFNPP requiring Entergy to fully implement and maintain in effect all provisions of the Commission-approved JAFNPP CSP as required by Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54, "Protection of digital computer and communication systems and networks." A *Federal Register* notice dated March 27, 2009, issued the final rule that amended 10 CFR Part 73. The regulations in 10 CFR 73.54, establish the requirements for a cyber security program. This regulation specifically requires each licensee currently licensed to operate a nuclear power plant under Part 50 of this chapter to submit a CSP that satisfies the requirements of the Rule. Each submittal must include a proposed implementation schedule and implementation of the licensee's CSP must be consistent with the approved schedule. The background for this application is addressed by the U.S. Nuclear Regulatory Commission (NRC) Notice of Availability, *Federal Register* Notice, Final Rule 10 CFR Part 73, Power Reactor Security Requirements, published on March 27, 2009 (74 FR 13926).

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 July 15, 2010, as supplemented by letters dated February 15, and 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.

V. P. Operations

- 2 -

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

Sincerely,

A handwritten signature in black ink that reads "B.K. Vaidya". The signature is written in a cursive style with a horizontal line underneath the name.

Bhalchandra K. Vaidya, Project Manager  
Plant Licensing Branch I-1  
Division of Operating Reactor Licensing  
Office of Nuclear Reactor Regulation

Docket No. 50-333

Enclosures:

1. Amendment No. 300 to DPR-59
2. Safety Evaluation

cc w/encls: Distribution via Listserv



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

ENERGY NUCLEAR FITZPATRICK, LLC

AND ENERGY NUCLEAR OPERATIONS, INC.

DOCKET NO. 50-333

JAMES A. FITZPATRICK NUCLEAR POWER PLANT

AMENDMENT TO RENEWED FACILITY OPERATING LICENSE

Amendment No. 300  
Renewed Facility Operating License No. DPR-59

1. The Nuclear Regulatory Commission (the Commission) has found that:
  - A. The application for amendment by Entergy Nuclear Operations, Inc. (the licensee) dated July 15, 2010, as supplemented by letters dated February 15, 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; 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 license is amended as indicated in the attachment to this license amendment, and paragraph 2.C.(2) of Renewed Facility Operating License No. DPR-59 is hereby amended to read as follows:

- (2) Technical Specifications

The Technical Specifications contained in Appendix A, as revised through Amendment No. 300, are hereby incorporated in the renewed operating license. The licensee shall operate the facility in accordance with the Technical Specifications.

Further, the following paragraph is added to the existing License Condition 2.D:

“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). ENO CSP was approved by License Amendment No. 300.”

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 July 15, 2010, as supplemented by letters dated February 15, and 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



Nancy L. Salgado, Chief  
Plant Licensing Branch I-1  
Division of Operating Reactor Licensing  
Office of Nuclear Reactor Regulation

Attachment:  
Changes to the Renewed Facility  
Operating License

Date of Issuance: August 19, 2011

ATTACHMENT TO LICENSE AMENDMENT

AMENDMENT NO. 300

RENEWED FACILITY OPERATING LICENSE NO. DPR-59

DOCKET NO. 50-333

Replace the following pages of the License with the attached revised pages. The revised pages are identified by amendment number and contain marginal lines indicating the areas of change.

Remove Pages

Page 3  
Page 5

Insert Pages

Page 3  
Page 5

- (4) ENO pursuant to the Act and 10 CFR Parts 30, 40, and 70 to receive, possess, and use, at any time, any byproduct, source and special nuclear material without restriction to chemical or physical form, for sample analysis or instrument calibration; or associated with radioactive apparatus, components or tools..
- (5) Pursuant to the Act and 10 CFR Parts 30 and 70, to possess, but not separate, such byproduct and special nuclear materials as may be produced by the operation of the facility.

C. This renewed operating license shall be deemed to contain and is subject to the conditions specified in the following Commission regulations in 10 CFR Chapter I: Part 20, Section 30.34 of Part 30, Section 40.41 of Part 40, Sections 50.54 and 50.59 of Part 50, and Section 70.32 of Part 70; and is subject to all applicable provisions of the Act and 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) Maximum Power Level

ENO is authorized to operate the facility at steady state reactor core power levels not in excess of 2536 megawatts (thermal).

(2) Technical Specifications

The Technical Specifications contained in Appendix A, as revised through Amendment No. 300, are hereby incorporated in the renewed operating license. The licensee shall operate the facility in accordance with the Technical Specifications.

(3) Fire Protection

ENO shall implement and maintain in effect all provisions of the approved fire protections program as described in the Final Safety Analysis Report for the facility and as approved in the SER dated November 20, 1972; the SER Supplement No. 1 dated February 1, 1973; the SER Supplement No. 2 dated October 4, 1974; the SER dated August 1, 1979; the SER Supplement dated October 3, 1980; the SER Supplement dated February 13, 1981; the NRC Letter dated February 24, 1981; Technical Specification Amendments 34 (dated January 31, 1978), 80 (dated May 22, 1984), 134 (dated July 19, 1989), 135 (dated September 5, 1989), 142 (dated October 23, 1989), 164 (dated August 10, 1990), 176 (dated January 16, 1992), 177 (dated February 10, 1992), 186 (dated February 19, 1993), 190 (dated June 29, 1993), 191 (dated July 7, 1993), 206 (dated February 28, 1994) and 214 (dated June 27, 1994); and NRC Exemptions and associated safety evaluations dated April 26, 1983, July 1, 1983, January 11, 1985, April 30, 1986, September 15, 1986 and September 10, 1992 subject to the following provision:

Safeguards Contingency Plan, Revision 0," submitted by letter dated October 26, 2004, as supplemented by letter dated May 17, 2006.

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). ENO CSP was approved by License Amendment No. 300.

E. Power Uprate License Amendment Implementation

The licensee shall complete the following actions as a condition of the approval of the power uprate license amendment.

(1) Recirculation Pump Motor Vibration

Perform monitoring of recirculation pump motor vibration during initial Cycle 13 power ascension for uprated power conditions.

(2) Startup Test Program

The licensee will follow a startup testing program, during Cycle 13 power ascension, as described in GE Licensing Topical Report NEDC-31897P-1, "Generic Guidelines for General Electric Boiling Water Reactor Power Uprate." The Startup test program includes system testing of such process control systems as the feedwater flow and main steam pressure control systems. The licensee will collect steady-state operational data during various portions of the power ascension to the higher licensed power level so that predicted equipment performance characteristics can be verified. The licensee will do the startup testing program in accordance with its procedures. The licensee's approach is in conformance with the test guidelines of GE Licensing Topical Report NEDC-31897P-1, "Generic Guidelines for General Electric Boiling Water Reactor Power Uprate." June 1991 (proprietary), GE Licensing Topical Report NEDO-31897, "Generic Guidelines for General Electric Boiling Water Reactor Power Uprate." February 1992 (nonproprietary), and NEDC-31897P-AA, Class III (proprietary), May 1992.

(3) Human Factors

The licensee will review the results of the Cycle 13 startup test program to determine any potential effects on operator training. Training issues identified will be incorporated in Licensed Operator training during 1997. Simulator discrepancies identified will be addressed in accordance with simulator Configuration Management procedural requirements.

F. Additional Conditions

The Additional Conditions contained in Appendix C, as revised through Amendment No. 289, are hereby incorporated into this renewed operating license. ENO shall operate the facility in accordance with the Additional Conditions.



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

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO AMENDMENT NO. 300 TO

RENEWED FACILITY OPERATING LICENSE NO. DPR-59

ENTERGY NUCLEAR OPERATIONS, INC.

JAMES A. FITZPATRICK NUCLEAR POWER PLANT

DOCKET NO. 50-333

1.0 INTRODUCTION

By letter dated July 15, 2010, Agencywide Documents Access and Management System (ADAMS) Accession No. ML102000012, as supplemented by letters dated February 15, and April 4, 2011 (ADAMS Accession Nos. ML110530205 and ML110950153, respectively), Entergy Nuclear Operations, Inc. (the licensee) submitted a request for changes to the James A. FitzPatrick Nuclear Power Plant (JAFNPP) Renewed Facility Operating License (FOL) for approval of the licensee's Cyber Security Plan (CSP) and Implementation Schedule for JAFNPP as required by Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54 (Reference 1). By letter dated April 4, 2011, the licensee supplemented their CSP (ADAMS Accession No. ML110950153), 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.

The supplements dated February 15, 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 published in the *Federal Register* (75 FR 51492).

The amendment would approve the CSP and associated implementation schedule, and revise Paragraph 2.D of FOL No. DPR-59 for JAFNPP 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."

## 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, 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 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.

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: NEI 08-09, "Cyber Security Plan Template, Revision 6), dated May 5, 2010 (ADAMS Accession No. ML101190371), 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 (Reference 4). The licensee submitted a CSP for the JAFNPP 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 15, 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.

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 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 3.24, 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 staff's 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 (ADAMS Accession No. ML102940009), 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 staff determined that this is defined as 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 required 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." The requirements of 10 CFR 73.54(a)(1) do not address protection of digital assets, computers or communication systems that provide "emergency planning" functions. The NRC asked for clarification on the use of the term "emergency planning" functions.

The licensee responded 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.

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.

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 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 CSP describes the defense-in-depth architecture as predicated on isolation of CDAs within levels 2, 3, and 4. Furthermore, data flows from lower levels to higher 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 requested further explanation on the characteristics, features and effectiveness of the hardware VPN. The licensee responded by letter dated February 15, 2011 (ADAMS Accession No. ML110530207) and stated that they would remove discussion of hardware VPN from Section 4.3 of the JAF CSP; Entergy plans to use a data diode or air gap to isolate CDAs. This was reflected in the updated CSP that was submitted on April 4, 2011 (ADAMS Accession No. ML110950153). By removing hardware VPN as a deterministic one-way isolation device from the defensive architecture, and using a data diode

or air gap to isolate CDAs, the licensee's defense-in-depth protective strategy discussion of deterministic devices is comparable to that of the one described in NEI 08-09, Revision 6.

In the CSP, the licensee substituted "Emergency Plan" functions for "Emergency Preparedness" functions (as defined in 10 CFR 73.54(a)(1)) in references to CDAs and CSs that would be protected via the submitted defense-in-depth architecture. The NRC staff requested 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" functions were protected under the submitted defense-in-depth architecture, as required by 10 CFR 73.54(a)(1). The licensee responded by letter dated February 15, 2011 (ADAMS Accession No. ML110530207) and stated that they would remove references to "Emergency Planning" and "Emergency Plan" in Section 4.3 of the JAF CSP and replace them with the term "Emergency Preparedness." This was reflected in the updated CSP that was submitted on April 4, 2011 (ADAMS Accession No. ML110950153). By replacing these terms, the NRC staff finds that the licensee's defense-in-depth protective strategy adequately addresses all of the systems within the scope of 10 CFR 73.54.

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" describes functions typically performed by data acquisition systems. The NRC staff finds this to be acceptable as per RG 5.71, Appendix C, Section C.7, which states, "CDAs that provide data acquisition functions are allocated at least defensive Level 3 protection."

This section is comparable to Regulatory Position C.3.2 and Appendix A, Section A.3.1.5 in RG 5.71.

Based on the above, the NRC staff finds that this section of the CSP submitted by the licensee 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.

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 (a) operating CDAs in a contingency, (b) roles and responsibilities of responders, (c) processes and procedures for backup and storage of information, (d) logical diagrams of network connectivity, (e) current configuration information, and (f) 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: 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.

### 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.

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.

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 3 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 (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 3 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. ML110950153), the licensee responded to the records retention issue using the language proposed by NEI in its letter dated February 28, 2011. Therefore, the staff finds this deviation from NEI 08-09, Revision 6 to be acceptable.

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 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 finds that the 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. ML110950153), 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.

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.

The NRC staff acknowledges that in its submittal dated July 15, 2011, as supplemented by letters dated February 15 and April 4, 2011, the licensee proposed several milestone dates for CSP implementation 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 thus will require prior NRC approval pursuant in 10 CFR 50.90.

### 3.23 Revision of the License Condition

In its submittal dated July 15, 2011, as supplemented by letters dated February 15 and April 4, 2011, the licensee proposed to add a paragraph to the license condition 2.D to require the licensee to fully implement and maintain in effect all the provisions of the NRC-approved CSP. The NRC staff modified licensee’s proposed license condition and the licensee agreed with the revised license condition proposed by the NRC staff.

The following paragraph is added to the existing License Condition 2.D:

“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). ENO CSP was approved by License Amendment No. 300.”

Based on the information in Section 3.0 of this safety evaluation and the modified license condition described above, the NRC concludes this as 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 3.21, “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 STATE CONSULTATION

In accordance with the Commission’s regulations, the New York State Energy Research and Development Authority (NYSERDA) was notified of the proposed issuance of a license amendments in response to the application by the licensee dated July 15, 2010, as

supplemented by letters dated February 15, and April 4, 2011, for the subject facilities in order to implement the CSP (ADAMS Package Accession No. ML111810087) as required by Title 10 of the Code of Federal Regulations (10 CFR) Section 73.54, "Protection of digital computer and communication systems and networks. On June 15, 2011 NYSERDA responded by email (ADAMS Package Accession No. ML111730139) to the NRC Office of Nuclear Regulatory Regulation (NRR). The response contained comments from the New York State Office of Cyber Security (OCS) following its review of the licensee's CSP, implementation schedule, and the licensee's responses to NRC requests for additional information. The OCS comments were based on a comparison of the licensee's CSP to the New York State Information Security Policy (PS03-002) and Information Classification and Control Policy and Standard (PS08-001). In these comments, OCS stated the PS03-002 and PS08-001 policies and standards are generic documents applicable to State agencies and do not include provisions for industrial facilities such as nuclear power plants.

## 5.1 Discussion

The licensee used the Nuclear Energy Institute (NEI) 08-09, Revision 6, cyber security plan template, which on May 5, 2010 the Nuclear Regulatory Commission (NRC) deemed acceptable for use in meeting the requirements Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54. The NEI 08-09, Revision 6, cyber security plan template is similar to the template provided in Appendix A of Regulatory Guide (RG) 5.71. The templates are based on cyber security standards put forth by the National Institute of Standards and Technology (NIST) and Department of Homeland Security (DHS), which were tailored by experts in cyber security, commercial nuclear power regulation, licensing and plant operations (including representatives from the NRC), the NEI, the nuclear power industry, and the private sector. The tailoring process focused on determining measures necessary to provide high assurance that critical plant functions at a nuclear power plant (NPP) are adequately protected against cyber attacks, up to and including the design basis threat (DBT). As a result, the cyber security policies and standards put forth by the NRC will differ from those developed by New York State. Once the licensee's cyber security plan is approved by the NRC, elements within this plan become a condition of its license. Furthermore, the plan requires the licensee to implement additional or more restrictive security controls if it is determined that further measures are necessary to successfully defend critical plant functions from cyber attacks (see Section C.3.3 Security Controls of RG 5.71).

The assets that fall within the scope of 10 CFR 73.54 include those digital computer and communication systems and networks associated with the following functions: safety and important-to-safety; security; emergency preparedness; and support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions. With regards to levels of specificity within the licensee's CSP, 10 CFR 73.54 is a performance-based regulation that focuses on desired, measurable outcomes, rather than prescriptive processes, techniques, or procedures. The level of specificity within the licensee's cyber security plan is sufficient for licensing. Additional specificity will be contained in site-specific policies and procedures, and supporting documentation associated with the implementation of security controls, which will be made available to NRC inspectors during on-site inspections and in the course of performing regulatory oversight activities.

For reasons specified in the OCS comments, implementation timeframes are a result of a variety of factors. Implementation of the cyber security controls specified within the respective

cyber security plans requires detailed planning and time. The milestone provided in the schedule represents the timeframe necessary for the licensee to determine the most effective approach for establishing the defensive architecture outlined in the cyber security plan without affecting the function of critical plant systems or the performance capability of structures, systems, and components relied upon to mitigate the consequences of postulated accidents. The actual approach taken will vary by licensee. In addition, security control implementation may require a plant outage before modifications to a critical digital asset are performed in an effort to avoid the disruption of critical plant functions, including safety, security, and emergency preparedness. Plant outages can further affect the implementation timeframe.

During the implementation period, the NRC continues to provide regulatory oversight while establishing its cyber security inspection program. Moreover, the NRC Cyber Assessment Team (CAT) is in place to coordinate with industry on security-related incidents, and to communicate to NPPs the vulnerability information necessary to aid in the development of protective strategies for defending against cyber attacks.

The NRC continuously seeks to improve the level of openness and transparency associated with its regulatory processes. Ensuring appropriate openness explicitly recognizes that the public must be informed about, and have a reasonable opportunity to participate meaningfully in, the NRC's regulatory processes. This openness and transparency is further supported through regular public meetings held by the NRC for the purpose of discussing topics such as cyber security. Information on public meetings is available on the NRC website (<http://www.nrc.gov/public-involve/public-meetings/meeting-schedule.html>).

## 5.2 NRC Staff Technical Responses

Although the responses provided below refer to sections within RG 5.71, the licensee used NEI 08-09 Revision 6 for their CSP. For regulatory consistency, the NRC technical staff has referred to sections within RG 5.71, however, there is in all cases a comparable section in NEI 08-09 Revision 6.

More detailed NRC staff technical responses to OCS comments are provided in Table 1 below.

**Table 1 Detailed Comment Responses**

<u>Report Page No.</u>	<u>Topic/Subject</u>	<u>NY State Comment</u>	<u>Response</u>
Page 3	Contrast between "Cyber Security Plan" and "Cyber Security Program"	Licensees are not required to submit policies, implementing procedures, site-specific analyses, or other supporting technical information to the NRC for prior review and approval as part of the cyber security plan. Such	NYS correctly observes that licensees are not required to submit this material for prior approval and that it will be made available for inspection by NRC staff. This is acceptable to the NRC staff because 10 CFR 73.54 is a performance-based rule, which affords licensees necessary flexibility in determining which measures will be taken to comply with the regulation. The detailed technical documentation resulting from the implementation of the licensees' cyber security program is maintained on-site by the licensee, and is available to the NRC during inspections. In other words, the cyber security plan outlines how the cyber security program will be

		information will only be made available for inspection by the NRC staff.	implemented and the program details will be maintained at the licensee's site.
Page 4	Comparison of NRC cyber security requirements to comparable requirements set forth by NY State OCS	New York State has no existing cyber security requirements applicable to industrial facilities such as nuclear power plants. As a result, comparison was made to the New York State information security policies and standards.	The scope of NY State's information security policy is very different from NRC's cyber regulation under 10 CFR 73.54, and associated guidance. ICS have different risks, priorities, reliability, and performance requirements than traditional IT systems. The NRC cyber security guidance (RG 5.71) includes a tailored security control baseline in accordance with guidance outlined in Section 3.3 of NIST SP 800-53, to include participation of experts from industry, NRC, and the private sector. Comparison of RG 5.71, which addresses cyber security at nuclear power plants, with other standards, such as NYS' standards, which were not intended to address industrial situations, will reveal substantial differences. These differences are justified by the difference between commercial or corporate needs and the needs of nuclear power plants.
Page 4	Principles of Confidentiality, Integrity, and Availability	PS08-001 states each information asset must be classified using three principles (confidentiality, integrity, and availability) and, based on this classification, certain controls must be implemented to secure the information asset.	<p>The NRC staff agrees that information must be managed based on confidentiality, integrity and availability and that appropriate controls must be implemented to secure information assets. 10 CFR 73.54(a)(2) and RG 5.71 Section C.2, Elements of a Cyber Security Plan, state licensees must protect critical plant systems within the scope of 10 CFR 73.54 from cyber attacks that would have the following effects:</p> <ul style="list-style-type: none"> <li>• adversely impact the integrity or confidentiality of data or software</li> <li>• deny access to or adversely impact the availability of systems, services, or data</li> <li>• adversely impact the operation of systems, networks, and associated equipment</li> </ul> <p>These three elements align with the principles of confidentiality, integrity, and availability as described by NY State.</p>
Page 4	Frequency of Access Control Policies and Procedures Reviews	PS08-001 Controls No. 1 and No. 47 require that agencies review all security procedures and controls, including the access control policy and procedures at least	<p>The NRC staff agrees that periodic cyber security program reviews are important in the face of changing threats. RG 5.71 Appendix C Section 4 states that continuous and ongoing monitoring and assessment of the complete security life cycle for CDAs provides a means to evaluate and manage cyber risk. This security lifecycle includes the following elements:</p> <ul style="list-style-type: none"> <li>• continuous monitoring and assessment,</li> <li>• configuration management,</li> </ul>

		<p>annually to ensure their effectiveness in the face of changing threats. 10 CFR 73.55(m) requires a review only every 24 months.</p>	<ul style="list-style-type: none"> <li>• change management,</li> <li>• security impact analysis of changes and environment,</li> <li>• effectiveness analysis,</li> <li>• ongoing assessment of security controls and programs effectiveness,</li> <li>• vulnerability scans/assessments,</li> <li>• change control, and</li> <li>• security program review.</li> </ul> <p>Based on a review of NIST, IEEE, DHS, and ISA standards, a multi-disciplinary team of industry, NRC, and private sector experts determined that twenty-four months represents an acceptable frequency for a complete program review, although, as stated above, there are continuous and ongoing monitoring and assessment activities focused on each of the CDAs at a licensee's facility.</p> <p>Furthermore, RG 5.71 states that a complete program review is required <i>at least</i> every 24 months, but also sets conditions for when such reviews would occur on a more frequent basis in Section C.4.3 Cyber Security Program Review.</p>
Page 4	Adequate Resources With Access to CDAs	<p>PS08-001 Control No. 6 requires agencies to ensure that more than one person has access to the CDA to ensure business continuity. This control could not be readily identified in the guidance, but may be part of the contingency plans that are part of the licensees' detailed cyber security programs.</p>	<p>The NRC staff agrees that having more than one person with access to a CDA (i.e., continuity) is an important part of a cyber security plan. Continuity is addressed by security control C.9.2 Contingency Plan in Appendix C of RG 5.71, which states that the licensee must document as part of the contingency plan the resources (in other words the people) needed for a potential crisis situation. In addition, security control C.9.3 Contingency Plan Testing states licensees will use realistic test/exercise scenarios and environments, including unscheduled system maintenance activities, such as responding to CDA components and system failures, as an opportunity to test or exercise the contingency plan. All of these aforementioned controls require that multiple people have access to all critical systems to include CDAs.</p>
Page 5	Media Control	<p>PS08-001 Control No. 9 requires that electronic storage media and devices be issued, owned, controlled, or approved by the</p>	<p>The NRC staff agrees that controlling electronic media is critical to maintaining high assurance against cyber attacks. Security Control C.1.1 Media Protection Policy and Procedures, Appendix C of RG 5.71, addresses control and protection of electronic storage media and devices. That security control states that the licensee must implement procedures for all associated media</p>

		<p>agency. This includes media used to record and store data, but not limited to tapes, hard drives, USB flash drives, memory cards/chips, CDs, and diskettes. This requirement is not specifically laid out in the media protection processes found in the guidance.</p>	<p>protection controls, including procedures for media receipt, storage, handling, sanitization, removal, use, and disposal. These procedures pertain to both digital and non-digital media.</p>
Page 5	Alternate Storage Sites	<p>PS08-001 Control No. 10 requires that agencies ensure the security of alternate storage sites. The guidance does not clearly provide for the review and approval of physical/cyber controls at alternate storage sites.</p>	<p>The NRC staff agrees that the security of off-site storage is important and addresses alternate storage site security by security control C.9.5 Alternate Storage Site and Location for Backups in Appendix C of RG 5.71. The description of this security control can be compared to the CP-6 Alternate Storage Site security control in NIST SP 800-53, Revision 3.</p>

Page 5	Transportation of Storage Media	PS08-001 Control No. 56 requires that executive management designate the level of management who can give written approval for transportation or storage of information outside of an approved storage facility and for transmission of information outside the agency. All such approvals must be documented by designated management. The guidance does not appear to require management review and/or approval of external systems used for storage/transmission. While this control could not be readily identified in the guidance, it may be part of the licensees' detailed cyber security programs.	Policies and procedures governing transportation or storage of information outside of an approved storage facility and for transmission of that information are part of the licensee's detailed cyber security program and will be available for NRC inspection on-site at the licensee facility.
Page 5	Media Protection	PS08-001 Control No. 13 requires the creation and implementation of written procedures to keep track of individual documents, files, devices, or media which contain sensitive data and the individuals who have possession of them. This control could not be readily	The NRC staff agrees that written procedures are important to maintaining a cyber security program and outlines the establishment of policies and procedures governing media protection in security control C.1.1 Media Protection Policy and Procedures, Appendix C, of RG 5.71. Media protection is part of the licensee's detailed cyber security program and will be available for NRC inspection on-site at the licensee facility.

		identified in the guidance, but may be part of the licensees' detailed cyber security programs.	
Page 5	Environmental	PS08-001 Control No. 21 requires information custodians to monitor environmental protection measures (e.g., HVAC, fire suppression) for problems and correct as needed. While the guidance includes implementation of environmental protection security controls (e.g., temperature, humidity), there is no mention of monitoring those controls to ensure they are functioning properly.	Because the environmental systems (e.g., HVAC) are not critical to the proper functioning of any of the safety systems, they are not addressed specifically by 10 CFR 73.54 or the RG 5.71. Nonetheless, the security control C.5.1 Physical and Environmental Protection Policies and Procedures in Appendix C of RG 5.71 does state that the licensees will develop procedures to facilitate the implementation of environmental protection policies and associated controls. This includes the security control C.5.3 Physical and Environmental Protection in that same section. In addition, continuous monitoring of all security controls is addressed in security control C.4.1 Continuous Monitoring and Assessment in Appendix C of RG 5.71.

Page 6	Password Complexity	<p>Guidance indicates that the length, strength, and complexity of passwords balance security and operational ease of access within the capabilities of the CDA. Given that these are CDAs, a minimum length should be specified. Under New York's Cyber Security Standard S10-004, User Password Management, the password length minimum is eight characters.</p>	<p>The NRC staff agrees that password management must balance security and operational considerations. However, password management represents a fundamental difference between IT systems and ICS at a nuclear power plant. In some cases, CDA passwords are hard coded into the system to meet process control (timing) requirements.</p> <p>However, in all cases, CDAs are protected by multiple levels of security (defense in depth), physical isolation, access control, and continuous monitoring. Furthermore, the RG 5.71 security control B.4.7 Authenticator Management in Appendix B provides guidance on password complexity and details will be documented in the licensees' on-site policies and procedures and made available to the NRC for inspections.</p>
Page 6	Structures, Systems, and Components (SSCs)	<p>To avoid confusion, the cyber security plans should be clarified to indicate that the controls apply to both CDAs and SSCs.</p>	<p>The NRC staff agrees that clarity is critical in a document as important as the licensee's cyber security plan and the plans have been clarified to indicate that systems, structures, and components (SSCs), are within the scope of 10 CFR 73.54. This clarification was in response to a letter dated November 26, 2010, wherein the NRC notified the North American Reliability Corporation (NERC) of a policy decision to include SSCs within the scope of 10 CFR 73.54. (See <a href="http://pbadupws.nrc.gov/docs/ML1031/ML103140394.pdf">http://pbadupws.nrc.gov/docs/ML1031/ML103140394.pdf</a>). However, not all SSCs are digital and would not be treated as a CDA. In other words, all SSCs are considered as input to the process to determine if a given device is a CDA. Controls are then applied to all CDAs, but not necessarily all SSCs.</p>
Page 6	Scope of Systems	<p>It is the view of New York State that the cyber security plans should be clarified to encompass all digital assets within the facilities, not just critical systems, to ensure the licensees address as many potential pathways for attack as possible.</p>	<p>The NRC staff agrees that CDA connectivity and all potential pathways (wired, wireless, or physical) should be addressed. 10 CFR 73.54(b)(1) requires licensees to analyze digital computer and communication systems and networks and identify those assets that must be protected against cyber attacks. Section C.3.1.4 Review and Validation in RG 5.71 states licensees will "confirm the direct and indirect connectivity of each CDA, and identify pathways to CDAs." This is to be accomplished by either physical walkdown inspection of each CDA's configuration and connections, or an electronic walkdown "if it is impractical to trace a communication pathway fully to its conclusion by means of a physical walkdown inspection."</p>

Page 6	Training	Training should be provided to all employees and contractors, not just designated appropriate personnel.	10 CFR 73.54(d)(1) requires licensees to ensure that all appropriate facility personnel are aware of cyber security requirements and receive training necessary to perform their assigned duties and responsibilities. Section C.10.2 Awareness Training, Appendix C, of RG 5.71 outlines additional role-based training that should be provided based on assigned roles and responsibilities, specific requirements identified by the defensive strategy, and CDAs to which personnel have authorized access. In addition, training activities are coordinated, and interdependent, with physical security training.
Page 7	Protection of Non-Digital Media	Cyber security plans should include the protection of information assets that can be used in a cyber attack. Information security controls should be applied to these information assets regardless of form or format. For example, paper documents containing blueprints for the plant should have confidentiality, availability, and integrity controls applied. It is possible that these controls are included in the licensees' physical protection programs and were, consequently, outside the scope of this review.	The NRC staff agrees that all information assets should be managed in accordance with the content contained therein. However, as noted in the NYS comment, the myriad other programs, policies, and procedures extant at all NPPs already address information assets in their various forms. Nonetheless, within the cyber security program the licensee is required to establish policies and procedures governing media protection as defined in security control C.1.1 Media Protection Policy and Procedures, Appendix C, of RG 5.71. Security control C.1.2 Media Access in this same section goes on to clarify that these procedures pertain to both digital and non-digital media. In addition to the protections outlined in RG 5.71, all licensee's must also comply with the requirement of 10 CFR 73.21 and 10 CFR 73.22 for the protection of Safeguards Information.
Page 7	Licensee Project Planning	While it is clear that the implementation of cyber security plans and programs at the facilities in question represents a large and complex undertaking, implementation schedules that	The NRC agrees that it is in the best interest of the licensees to ensure that project plans address those items outlined in the comment. Detailed project plans with a greater level of specificity will be developed by the licensees for completion of milestones identified in the implementation schedules. Any deviation from the implementation schedule requires the licensee to request and receive approval from the NRC, under 10 CFR 50.90.  The NRC staff believes that setting deadlines for

		<p>identify the latest possible dates for the completion of all milestones are not indicative of a rational approach to project management. Establishing an implementation schedule that includes reasonable risk, effort, and resource based dates for the completion of individual key intermediate milestones would appear to be essential to managing such an undertaking.</p>	<p>implementation of the various facets of the CSP is essential to achieving full implementation in a timely fashion. Licensees' implementation schedules also serve a practical licensing purpose; the NRC obtains assurance from licensees as to when certain cyber security program elements will be in place and the NRC can then schedule on-site inspection activities.</p>
<p>Page 7/8</p>	<p>Implementation dates</p>	<p>It is our view that full implementation of the cyber security plans should be completed sooner than the dates identified in the current implementation schedules. These dates, which are three to four years in the future, do not appropriately reflect the gravity of the cyber security risks that confront these critical facilities.</p>	<p>The NRC agrees that full implementation of the cyber security program should be completed as soon as possible. The intent of the implementation schedule is to complete a majority of the cyber-significant work by the end of 2012. The first seven milestones are:</p> <ul style="list-style-type: none"> <li>• building the Cyber Security Assessment Team (CSAT),</li> <li>• identifying the Critical Systems (CSs) and Critical Digital Assets (CDAs),</li> <li>• isolating Levels 3 &amp; 4 (where the most important systems are located),</li> <li>• controlling portable and mobile devices,</li> <li>• looking for obvious cyber tampering,</li> <li>• applying security controls to at least the CDAs,</li> <li>• implementation of continuous monitoring of those CDAs and their respective controls.</li> </ul> <p>The three to four years for full implementation of the cyber security program reflects the complexity of the issues involved. Furthermore, some of the cyber security program elements will require work that can only be accomplished during a shut-down or refueling outage. For multi-unit (multi-reactor) sites this may require several years to fully implement all cyber security program elements.</p>

<p>Page 8/9</p>	<p>No Significant Hazard Determination</p>	<p>In their implementation schedules, all licensees state that "[i]solating the plant systems from the internet, as well as from the corporate business systems is an important milestone in defending against external threats. While the deployment of the barriers is critical to protection from external cyber threats, it also prevents remote access to core monitoring and plant data systems for reactor engineers, plant operations, and other plant staff. This elimination of remote access to reactor core monitoring systems may require the development and execution of a detailed change management plan to ensure continued safe operation of the plants." This statement appears to be inconsistent with the NRC's finding that the amendment will not involve a significant increase in the probability or consequences of an accident previously evaluated; or (2) create the possibility of a new or different</p>	<p>As stated in 10 CFR 73.54, licensees are required to protect critical plant systems from cyber attacks, up to and including the DBT. Isolation of critical plant systems from the Internet and corporate IT systems is part of the security defensive architecture and defense-in-depth strategies described in RG 5.71.</p> <p>Isolating plant systems from the Internet and corporate business systems will not interfere with the ability of engineers in the control room to monitor the core or other critical safety functions.</p> <p>Implementation of a detailed change management plan as an alternative control for allowing remote maintenance access to CDAs is acceptable, as long as the alternative control does not adversely impact SSEP functions.</p>
---------------------	--	--	--

		kind of accident from any accident previously evaluated; or (3) involve a significant reduction in a margin of safety.	
Page 9	General Recommendations	<p>It is imperative that cyber security be made a priority. While the creation of cyber security plans is an important first step, programs need to be in place to ensure that these plans are implemented at an appropriate pace, and once implemented are followed. In addition, it is also important for the licensees to provide transparency for their efforts to mitigate cyber security vulnerabilities while they are progressing toward full implementation of the required cyber security plans. Finally, OCS recommends that the implementation of the cyber security plans be substantiated by NRC inspections.</p>	<p>The NRC staff agrees that cyber security is a priority, that plans must be created and implemented at an appropriate pace and must be followed and inspected, and that transparency should be promoted so long as it does not jeopardize safety or security.</p> <p>Every NPP has its own implementation schedule, but there are unifying elements across the operating fleet's documentation. The intent of the implementation schedule is to complete a majority of the cyber-significant work by the end of 2012 and the final milestone includes the completion of all remaining actions that result in the full implementation of the cyber security program for all applicable safety, security, and emergency preparedness functions.</p> <p>While the NRC completes the reviews of the licensee's cyber security plans, the NRC Oversight and Inspection program is preparing for on-site inspections.</p>

6.0 ENVIRONMENTAL CONSIDERATION

The amendment, by incorporation of the NRC-approved CSP and the NRC-approved CSP implementation schedule in the licensing basis, involves (1) changes in a requirement with respect to installation or use of a facility component located within the restricted area as defined in 10 CFR Part 20, (2) changes in record keeping, reporting, or administrative procedures or requirements, and (3) solely related to safeguards matters (protection against sabotage) involving (a) Organizational and Procedural matters, (b) Modifications to systems used for

security, and (c). Administrative changes. The NRC staff has determined that the amendment involves no significant increase in amounts, 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. On August 20, 2010, the Commission published its proposed finding that the amendments involve no significant hazards consideration (75 FR 62492). There were no public comments on that proposed finding within thirty days of publication. While New York State filed a number of comments on the CSP approximately nine months later, on June 15, 2011, it did not comment on the proposed no significant hazards consideration within thirty days of publication of the proposed finding in the *Federal Register*. 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 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 JAFNPP will not be inimical to the common defense and security. 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.

## 8.0 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. Regulatory Guide 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: J. Green, NSIR/CSIRB

Date: August 19, 2011

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

Sincerely,

*/ra/*

Bhalchandra K. Vaidya, Project Manager  
 Plant Licensing Branch I-1  
 Division of Operating Reactor Licensing  
 Office of Nuclear Reactor Regulation

Docket No. 50-333

Enclosures:

1. Amendment No. 300 to DPR-59
2. Safety Evaluation

cc w/encls: Distribution via Listserv

**DISTRIBUTION:**

PUBLIC LPL1-1 R/F RidsNrrDorLPL1-1 RidsOGCMailCenter RidsNrrDirsltsb  
 RidsAcrsAcnwMailCenter RidsNsrDsplscpb RidsNrrPMFitzPatrick  
 P. Pederson, NSIR/CSIRB RidsNrrLASLittle (paper copy)  
 MGray, RI J. Green, NSIR/CSIRB

**ADAMS Accession No.: ML11152A011 (\*) No substantial change from SE Input Memo**

OFFICE	LPL1-1\PM	LPL1-1\LA	NRC/NSIR/DSP/CSIRB/BC	OGC (NLO w/ comment)	LPL1-1\BC	LPL1-1\PM
NAME	BVaidya	SLittle	CErlanger (*)	AJones	NSalgado	BVaidya
DATE	08/01/11	08/02/11	06/23/11 and 07/09/11	08/18/11	08/19/11	08/19/11

**Official Record Copy**