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

July 21, 2011

Mr. Timothy S. Rausch
Senior Vice President and Chief Nuclear Officer
PPL Susquehanna, LLC
769 Salem Boulevard
Berwick, PA 18603-0467

SUBJECT: SUSQUEHANNA STEAM ELECTRIC STATION, UNITS 1 AND 2 - ISSUANCE OF AMENDMENT RE: APPROVAL OF THE PPL SUSQUEHANNA, LLC CYBER SECURITY PLAN (TAC NOS. ME4420 AND ME4421)

Dear Mr. Rausch:

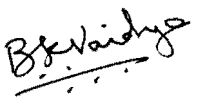
The Commission has issued the enclosed Amendment No. 255 to Renewed Facility Operating License No. NPF-14 and Amendment No. 235 to Renewed Facility Operating License No. NPF-22 for the Susquehanna Steam Electric Station (SSES), Units 1 and 2. These amendments consist of changes to the Renewed Facility Operating Licenses (FOLs) in response to your application dated, July 22, 2010, as supplemented by letter dated April 4, 2011.

The request for the amendments to the Renewed FOLs include: (1) the proposed SSES Units 1 and 2 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 SSES Units 1 and 2 requiring PPL Susquehanna, LLC to fully implement and maintain in effect all provisions of the Commission-approved SSES Units 1 and 2 Cyber Security Plan 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 cyber security plan that satisfies the requirements of the Rule. Each submittal must include a proposed implementation schedule and implementation of the licensee's Cyber Security Program 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).

These license amendments are 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 22, 2010, as supplemented by letter dated 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.

A copy of our safety evaluation is also enclosed. Notice of Issuance will be included in the Commission's next regular Biweekly *Federal Register* Notice.

Sincerely,



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

Docket Nos. 50-387 and 50-388

Enclosures:
1. Amendment No. 255 to License No. NPF-14
2. Amendment No. 235 to License No. NPF-22
3. Safety Evaluation

cc w/encls: Distribution via Listserv

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

PPL SUSQUEHANNA, LLC

ALLEGHENY ELECTRIC COOPERATIVE, INC.

DOCKET NO. 50-387

SUSQUEHANNA STEAM ELECTRIC STATION, UNIT 1

AMENDMENT TO RENEWED FACILITY OPERATING LICENSE

Amendment No. 255
License No. NPF-14

1. The Nuclear Regulatory Commission (the Commission or the NRC) having found that:

   A. The application for the amendment filed by PPL Susquehanna, LLC, dated July 22, 2010, as supplemented by letter dated April 4, 2011, complies with the standards and requirements of the Atomic Energy Act of 1954, as amended (the Act), and the Commission's 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 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 set forth in 10 CFR Chapter I;

   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 by changes as indicated in the attachment to this license amendment and paragraphs 2.C.(2) of the Renewed Facility Operating License No. NPF-14 are hereby amended to read as follows:

   (2) Technical Specifications and Environmental Protection Plan

   The Technical Specifications contained in Appendix A, as revised through Amendment No. 255 and the Environmental Protection Plan contained in Appendix B, are hereby incorporated in the license. PPL Susquehanna, LLC shall operate the facility in accordance with the Technical Specifications and the Environmental Protection Plan.

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

   "The operating licensee 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 PPL Susquehanna, LLC CSP was approved by License Amendment No. 255."

3. 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 by letter July 22, 2010, as supplemented by letter dated 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

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

Attachment:
Changes to the License

Date of Issuance: July 21, 2011

ATTACHMENT TO LICENSE AMENDMENT NO. 255

RENEWED FACILITY OPERATING LICENSE NO. NPF-14

DOCKET NO. 50-387

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

REMOVE	INSERT
Page 3	Page 3
Page 19	Page 19

(3) PPL Susquehanna, LLC, 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 as sealed neutron sources for reactor startup, sealed neutron sources for reactor instrumentation and radiation monitoring equipment calibration, and as fission detectors in amounts as required;

(4) PPL Susquehanna, LLC, 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 without restriction to chemical or physical form, for sample analysis or instrument calibration or associated with radioactive apparatus or components; and

(5) PPL Susquehanna, LLC, 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 operation of the facility.

C. This license shall be deemed to contain and is subject to the conditions specified in the Commission's regulations set forth in 10 CFR Chapter I 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

PPL Susquehanna, LLC is authorized to operate the facility at reactor core power levels not in excess of 3952 megawatts thermal in accordance with the conditions specified herein. The preoperational tests, startup tests and other items identified in License Conditions 2.C.(36), 2.C.(37), 2.C.(38), and 2.C.(39) to this license shall be completed as specified.

(2) Technical Specifications and Environmental Protection Plan

The Technical Specifications contained in Appendix A, as revised through Amendment No. 255 and the Environmental Protection Plan contained in Appendix B are hereby incorporated in the license. PPL Susquehanna, LLC shall operate the facility in accordance with the Technical Specifications and the Environmental Protection Plan.

For Surveillance Requirements (SRs) that are new in Amendment 178 to Facility Operating License No. NPF-14, the first performance is due at the end of the first surveillance interval that begins at implementation of Amendment 178. For SRs that existed prior to Amendment 178, including SRs with modified acceptance criteria and SRs whose frequency of performance is being extended, the first performance is due at the end of the first surveillance interval that begins on the date the Surveillance was last performed prior to implementation of Amendment 178.

(38) Neutronic Methods

(a) An OPRM amplitude setpoint penalty will be applied to account for a reduction in thermal neutrons around the LPRM detectors caused by transients that increase voiding. This penalty will reduce the OPRM scram setpoint according to the methodology described in Response No. 3 of PPL letter, PLA-6306, dated November 30, 2007. This penalty will be applied until NRC evaluation determines that a penalty to account for this phenomenon is not warranted.

(b) For SSES SLMCPR, a conservatively adjusted pin power distribution uncertainty and bundle power correlation coefficient will be applied as stated in Response No. 4 of PPL letter, PLA-6306, dated November 30, 2007, when performing the analyses in accordance with ANF-524(P)(A), "Critical Power Methodology for Boiling Water Reactors," using the uncertainty parameters associated with EMF-2158(P)(A) "Siemens Power Corporations Methodology for Boiling Water Reactors: Evaluation and Validation of CASMO-4/MICROBURN-B2. "

(39) Containment Operability for EPU

PPL shall ensure that the CPPU containment analysis is consistent with the SSES 1 and 2 operating and emergency procedures. Prior to operation above CLTP, for each respective unit, PPL shall notify the NRC project manager that all appropriate actions have been completed.

(40) Primary Containment Leakage Rate Testing Program

Those primary containment local leak rate program tests (Type B - leakage-boundary and Type C - containment isolation valves) as modified by approved exemptions, required by 10 CFR Part 50, Appendix J, Option B and Technical Specification 5.5.12, are not required to be performed at the CPPU peak calculated containment internal pressure of 48.6 psig (Amendment No. 246 to this Operating License) until their next required performance.

D. The operating licensee 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 plan, which contains Safeguards Information protected under 10 CFR 73.21, is entitled: "Physical Security Plan, Training and Qualification Plan, Safeguards Contingency Plan and Security and Contingency Plan for Independent Spent Fuel Storage Facility," and was submitted October 8, 2004.

The operating licensee 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 PPL Susquehanna, LLC CSP was approved by License Amendment No. 255.

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

PPL SUSQUEHANNA, LLC

ALLEGHENY ELECTRIC COOPERATIVE, INC.

DOCKET NO. 50-388

SUSQUEHANNA STEAM ELECTRIC STATION, UNIT 2

AMENDMENT TO RENEWED FACILITY OPERATING LICENSE

Amendment No. 235
License No. NPF-22

1. The Nuclear Regulatory Commission (the Commission or the NRC) having found that:

   A. The application for the amendment filed by the PPL Susquehanna, LLC, dated July 22, 2010, as supplemented by letter dated April 4, 2011, complies with the standards and requirements of the Atomic Energy Act of 1954, as amended (the Act), and the Commission's 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 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 set forth in 10 CFR Chapter I;

   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 by changes as indicated in the attachment to this license amendment and paragraph 2.C.(2) of the Renewed Facility Operating License No. NPF-22 is hereby amended to read as follows:

(2) Technical Specifications and Environmental Protection Plan

The Technical Specifications contained in Appendix A, as revised through Amendment No. 235 and the Environmental Protection Plan contained in Appendix B, are hereby incorporated in the license. PPL Susquehanna, LLC shall operate the facility in accordance with the Technical Specifications and the Environmental Protection Plan.

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

"The operating licensee 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 PPL Susquehanna, LLC CSP was approved by License Amendment No. 235."

3. 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 by letter July 22, 2010, as supplemented by letter dated 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

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

Attachment:
Changes to the License

Date of Issuance: July 21, 2011

ATTACHMENT TO LICENSE AMENDMENT NO. 235

RENEWED FACILITY OPERATING LICENSE NO. NPF-22

DOCKET NO. 50-388

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

REMOVE	INSERT
Page 3	Page 3
Page 15	Page 15

(3) PPL Susquehanna, LLC, 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 as sealed neutron sources for reactor startup, sealed neutron sources for reactor instrumentation and radiation monitoring equipment calibration, and as fission detectors in amounts as required;

(4) PPL Susquehanna, LLC, 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 without restriction to chemical or physical form, for sample analysis or instrument calibration or associated with radioactive apparatus or components; and

(5) PPL Susquehanna, LLC, 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 operation of the facility.

C. This license shall be deemed to contain and is subject to the conditions specified in the Commission's regulations set forth in 10 CFR Chapter I 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

PPL Susquehanna, LLC is authorized to operate the facility at reactor core power levels not in excess of 3952 megawatts thermal in accordance with the conditions specified herein. The preoperational test, startup tests and other items identified in License Conditions 2.C.(20), 2.C.(21), 2.C.(22), and 2.C.(23) to this license shall be completed as specified.

(2) Technical Specifications and Environmental Protection Plan

The Technical Specifications contained in Appendix A, as revised through Amendment No. 235 and the Environmental Protection Plan contained in Appendix B, are hereby incorporated in the license. PPL Susquehanna, LLC shall operate the facility in accordance with the Technical Specifications and the Environmental Protection Plan.

For Surveillance Requirements (SRs) that are new in Amendment 151 to Facility Operating License No. NPF-22, the first performance is due at the end of the first surveillance interval that begins at implementation of Amendment 151. For SRs that existed prior to Amendment 151, including SRs with modified acceptance criteria and SRs whose frequency of performance is being extended, the first performance is due at the end of the first surveillance interval that begins on the date the Surveillance was last performed prior to implementation of Amendment 151.

(25) Critical Power Correlation Additive Constants

AREVA NP has submitted EMF-2209(P), Revision 2, Addendum 1 (ML081260442) for NRC review to correct the critical power correlation additive constants due to a prior Part 21 notification (ML072830334). The report is currently under NRC review.

The license shall apply additional margin to the cycle specific OLMCPR, consistent in magnitude with the non-conservatism reported in the Part 21 report, thus imposing the appropriate MCPR penalty on the OLMCPR. This compensatory measure is to be applied until the approved version of EMF-2209(P), Revision 2, Addendum 1 is published and PPL verifies that the additive constants from the approved report have been incorporated in the cycle specific analyses.

D. The operating licensee 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 plan, which contains Safeguards Information protected under 10 CFR 73.21, is entitled: "Physical Security Plan, Training and Qualification Plan, Safeguards Contingency Plan and Security and Contingency Plan for Independent Spent Fuel Storage Facility," and was submitted October 8, 2004.

The operating licensee 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 PPL Susquehanna, LLC CSP was approved by License Amendment No. 235.

E. DELETED

F. PPL Susquehanna, LLC 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.

G. The information in the Updated Final Safety Analysis Report (UFSAR) supplement, as revised, submitted pursuant to 10 CFR 54.21(d), shall be incorporated into the UFSAR no later than the next scheduled update required by 10 CFR 50.71(e) following the issuance of this renewed operating license. Until this update is complete, PPL Susquehanna, LLC may not make changes to the information in the supplement. Following incorporation into the UFSAR, the need for prior Commission approval of any changes will be governed by 10 CFR 50.59.

H. The UFSAR supplement, as revised, submitted pursuant to 10 CFR 54.21(d), describes certain future activities to be completed prior to and/or during the period of extended operation. The licensee shall complete these activities in accordance with Appendix A of NUREG-1931, "Safety Evaluation Report Related to the Susquehanna Steam Electric Station, Units 1 and 2," dated November, 2009. The licensee shall notify the NRC in writing when activities to be completed prior to the period of extended operation are complete and can be verified by NRC inspection.

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

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO

AMENDMENT NO 255 TO RENEWED FACILITY OPERATING LICENSE NO. NPF-14 AND

AMENDMENT NO. 235 TO RENEWED FACILITY OPERATING LICENSE NO. NPF-22

PPL SUSQUEHANNA, LLC

ALLEGHENY ELECTRIC COOPERATIVE, INC.

SUSQUEHANNA STEAM ELECTRIC STATION, UNITS 1 AND 2

DOCKET NOS. 50-387 AND 50-388

1.0 INTRODUCTION

By application dated July 22, 2010 (Agencywide Documents Access and Management System (ADAMS) Package Accession No. ML102150151), as supplemented by letter dated April 4, 2011 (ADAMS Package Accession No. ML111020217), PPL Susquehanna, LLC (the licensee), requested changes to the Renewed Facility Operating Licenses (FOLs) for Susquehanna Steam Electric Station, Units 1 and 2 (SSES-1 and -2) for approval of the licensee's Cyber Security Plan (CSP) and Implementation Schedule for the Susquehanna Steam Electric Station, Units 1 and 2 as required by Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54, "Protection of digital computer and communication systems and networks," (Reference 1). By letter dated April 4, 2011, the licensee supplemented their CSP 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 request for additional information (RAI) responses.

The supplement dated 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 staff's original proposed no significant hazards consideration determination as published in the *Federal Register* on October 12, 2010 (75 FR 62606).

The amendments would approve the CSP and associated implementation schedule, and revise Paragraph 2.D of FOL Nos. NPF-14 and NPF-22 for SSES-1 and SSES-2, respectively, to provide the license conditions 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 cyber security plan which licensees may use to comply with the licensing requirements of 10 CFR 73.54. Appendices B and C provide an acceptable set of security controls, which are based on well-understood threats, vulnerabilities, and attacks, coupled with equally well-understood and vetted countermeasures and protective techniques.

NEI 08-09, Revision 6 closely maps with RG 5.71; Appendix A of NEI 08-09, Revision 6 contains a cyber security plan 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 (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 Susquehanna Steam Electric Station that was based on the template provided in NEI 08-09, Revision 6 and included a definition of cyber attack acceptable to the NRC staff in the deviation table (Table 1) submitted with the CSP. 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 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 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 NRC staff determined that those systems that have a nexus to radiological health and safety 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 NRC staff reviewed the CSP and the supplemental information submitted by the licensee and found no deviation from Regulatory Position C.3.3 in RG 5.71 and Appendix A, Section A.2.1 of RG 5.71. The NRC staff finds that the licensee established adequate measures to implement and document the Cyber Security Program, including baseline security controls.

Based on the above, the NRC staff finds that the 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 describes 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 concludes that the licensee established adequate measures to define and address the purpose, scope, roles, responsibilities, management commitment, and coordination, and facilitates 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 in 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 describes 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 walk downs. 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.

This section of the CSP submitted by the licensee is comparable to Regulatory Position C.3.3 in RG 5.71 and Appendix A, Section A.3.1.6 without deviation. This section of the CSP submitted by the licensee is also comparable to Regulatory Position C.3.3 in RG 5.71 without deviation.

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 describes 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.

This section of the CSP submitted by the licensee is comparable to Regulatory Position C.3.2 and Appendix A, Section A.3.1.5 in RG 5.71 without deviation.

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 (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.

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.

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 positions 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 described 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 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 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. ML111020207), the licensee responded to the records retention RAI 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 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. ML111020207), 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 22, 2010, as supplemented by letter dated April 4, 2011, the licensee proposed several mile stones 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 22, 2010, the licensee proposed to add a paragraph to the existing License Condition 2.D in each license.

The following paragraph is added to the existing License Condition 2.D in each Renewed Facility Operating License for Susquehanna Units 1 and 2:

(1) For Susquehanna Unit 1: "The operating licensee 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 PPL Susquehanna, LLC CSP was approved by License Amendment No. 255."

(2) For Susquehanna Unit 2: "The operating licensee 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 PPL Susquehanna, LLC CSP was approved by License Amendment No. 235."

Based on the information in Section 3.0 of this SE and the revised license condition described above, the NRC concludes that this is acceptable.

3.24 Differences from NEI 08-09, Revision 6

In addition to the table of deviations found in Table 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 3.21, "Document Control and Records Retention and Handling," the licensee clarified the definition of records and supporting documentation that will be retained to conform to the requirements of 10 CFR 73.54.

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

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

3.25 Conclusion – Technical Evaluation

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 Susquehanna Steam Electric Station will not be inimical to the common defense and security.

4.0 STATE CONSULTATION

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

5.0 ENVIRONMENTAL CONSIDERATION

The amendments, by incorporation of the NRC-approved CSP and the NRC-approved CSP implementation schedule in the licensing basis, involve (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 and changes surveillance requirements , (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 amendments involve 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. The Commission has previously issued a proposed finding that the amendments involve no significant hazards consideration, and there has been no public comment on such finding (75 FR 62606). 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.

6.0 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 amendments will not be inimical to the common defense and security or to the health and safety of the public.

7.0 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: R. Spitzberg, NSIR/DSP/ISCPB

Date: July 21, 2011

A copy of our safety evaluation is also enclosed. 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 Nos. 50-387 and 50-388

Enclosures:
1. Amendment No. 255 to License No. NPF-14
2. Amendment No. 235 to License No. NPF-22
3. Safety Evaluation

cc w/encls: Distribution via Listserv

DISTRIBUTION:

PUBLIC LPL1-1 R/F	RidsNRRDorlLPl1-1	RidsNRRPMSusquehanna
RidsNrrLASLittle (hard copy)	RidsOGCMailCenter	RidsNsirDspIscpb
RidsNrrDorlDpr	RidsNrrDirsItsb	RidsAcrsAcnw&mMailCenter
RidsRg1MailCenter	PKrohn, RI	P. Pederson, NSIR/DSP/ISCPB
R. Spitzberg, NSIR/DSP/ISCPB		

ADAMS Accession No.: ML11152A009 (*)no substantial changes in SE Input Memo

OFFICE	LPL1-1/PM	LPL1-1/LA	NRC/NSIR/DSP/ISCPB/BC	OGC (NLO w/ comments)	LPL1-1/BC	LPL1-1/PM
NAME	BVaidya	SLittle	CErlanger (*)	AJones	NSalgado	BVaidya
DATE	06/24/11	06/22/11	06/01/11 and 07/09/11	07/11/11	07/21/11	07/21/11

OFFICIAL RECORD COPY