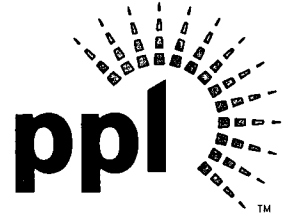


**Timothy S. Rausch**  
Sr. Vice President & Chief Nuclear Officer

**PPL Susquehanna, LLC**  
769 Salem Boulevard  
Berwick, PA 18603  
Tel. 570.542.3445 Fax 570.542.1504  
tsrausch@pplweb.com



JUL 22 2010

U.S. Nuclear Regulatory Commission  
Attn: Document Control Desk  
Mail Stop OP1-17  
Washington, DC 20555

**SUSQUEHANNA STEAM ELECTRIC STATION  
PROPOSED AMENDMENT NO. 306 TO LICENSE  
NPF-14 AND PROPOSED AMENDMENT NO. 277  
TO LICENSE NPF-22: WITHDRAWAL AND  
RESUBMITTAL OF REQUEST FOR APPROVAL OF THE  
PPL SUSQUEHANNA, LLC CYBER SECURITY PLAN  
PLA-6628**

**Docket Nos. 50-387  
and 50-388**

*Reference: (1) Letter from PPL (T. S. Rausch) to NRC Document Control Desk,  
"Susquehanna Steam Electric Station Proposed Amendment No. 306  
to License NPF-14 and Proposed Amendment No. 277 to License NPF-22:  
Request for Approval of the PPL Susquehanna, LLC Cyber Security Plan,"  
dated November 16, 2009.*

*(2) Letter from PPL (T. S. Rausch) to NRC Document Control Desk,  
"Susquehanna Steam Electric Station Proposed Amendment No. 306  
to License NPF-14 and Proposed Amendment No. 277 to License NPF-22:  
Supplement to Request for Approval of the PPL Susquehanna, LLC Cyber  
Security Plan," dated January 5, 2010.*

*(3) Letter from NRC (Richard V. Guzman) to PPL (Mr. Timothy S. Rausch),  
Susquehanna Steam Electric Station, Unit Nos. 1 and 2 – PPL Susquehanna, LLC  
RE: Cyber Security Plan License Amendment Request (TAC Nos. ME2649 and  
ME2650), dated May 27, 2010.*

PPL Susquehanna, LLC (PPL) submitted a request for an amendment to the Facility Operating Licenses (FOL) for Susquehanna Steam Electric Station, Units 1 and 2 in Reference (1) and supplemented the request in Reference (2). In Reference (3), the NRC noted that the Susquehanna request was based on a version of the NEI 08-09 guidance with which the NRC had significant generic concerns. Reference (3) also noted that a subsequent version of NEI 08-09 (Revision 6) was acceptable to the NRC with the exception of the definition of "cyber attack".

SDOIA  
MLL

The purpose of this letter is to withdraw the request for amendment submitted in Reference (1) and supplemented in Reference (2) and to submit a revised request for amendment. This revised request submits a Cyber Security Plan that is consistent with NEI 08-09, Revision 6 with the exception that the definition of "cyber attack" has been changed to maintain alignment with agreements reached with the NRC staff. This revised submittal replaces, in its entirety, the previous submittals.

In accordance with the provisions of 10 CFR §50.4 and §50.90, PPL Susquehanna, LLC (PPL) is submitting this request for an amendment to the Facility Operating Licenses (FOL) for Susquehanna Steam Electric Station, Units 1 and 2.

The proposed amendment requests NRC approval of the PPL Susquehanna, LLC Cyber Security Plan, provides an Implementation Schedule, and adds a sentence to the existing FOL Physical Protection license condition to require PPL to fully implement and maintain in effect all provisions of the Commission-approved Cyber Security Plan.

These proposed changes have been reviewed by both the Plant Operations Review Committee (PORC) and the Susquehanna Review Committee (SRC).

Enclosure 1 provides an evaluation of the proposed change. Enclosure 1 also contains the following attachments:

- Attachment 1 provides the existing FOL page for Unit 1 marked up to show the proposed change.
- Attachment 2 provides the existing FOL page for Unit 2 marked up to show the proposed change.

Enclosure 2 provides a copy of the PPL Susquehanna, LLC Cyber Security Plan Implementation Schedule. This schedule and its associated actions represent a new regulatory commitment. The schedule and associated commitment are contingent upon NRC approval of the PPL Susquehanna, LLC Cyber Security Plan by July 31, 2011.

Enclosure 3 provides a copy of the PPL Susquehanna, LLC Cyber Security Plan which is a stand-alone document that will be incorporated by reference into the PPL Physical Security Plan upon approval. PPL requests that Enclosure 3, which contains security-related sensitive information, be withheld from public disclosure in accordance with 10 CFR 2.390.

In accordance with 10 CFR 50.91, a copy of this application, with attachments, is being provided to the designated Commonwealth of Pennsylvania state official.

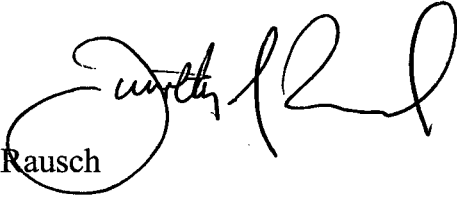
PPL requests an implementation period in accordance with the implementation schedule in Enclosure 2 (i.e., by December 1, 2015).

If you should have any questions regarding this submittal, please contact Mr. Michael Crowthers at (610) 774-7766.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: 7/22/10

T. S. Rausch

A handwritten signature in black ink, appearing to read "T. S. Rausch", written over a circular stamp or mark.

Enclosures:

1. Evaluation of Proposed Change
2. PPL Susquehanna, LLC Cyber Security Plan Implementation Schedule
3. PPL Susquehanna, LLC Cyber Security Plan [Security-Related Information – Withhold Under 10 CFR 2.390]

Attachments to Enclosure 1:

1. Facility Operating License, Unit 1 (Mark-up)
2. Facility Operating License, Unit 2 (Mark-up)

cc: NRC Region I  
Mr. P. W. Finney, NRC Sr. Resident Inspector  
Mr. R. V. Guzman, NRC Sr. Project Manager  
Mr. R. R. Janati, DEP/BRP

---

## **Enclosure 1 to PLA-6628**

# **Evaluation of Proposed Change Request for Approval of the PPL Susquehanna, LLC Cyber Security Plan**

---

1. Summary Description
2. Detailed Description
3. Technical Evaluation
4. Regulatory Evaluation
  - 4.1 Applicable Regulatory Requirements / Criteria
  - 4.2 Significant Hazards Consideration
  - 4.3 Conclusion
5. Environmental Consideration
6. References

### **ATTACHMENTS:**

Attachment 1 – Facility Operating License, Unit 1 (Mark-up)

Attachment 2 – Facility Operating License, Unit 2 (Mark-up)

## PPL EVALUATION

**Subject: PPL Evaluation of Proposed Change to the Unit 1 and Unit 2 Request for Approval of the PPL Susquehanna, LLC Cyber Security Plan**

### **1. SUMMARY DESCRIPTION**

The proposed license amendment request includes the proposed PPL Susquehanna, LLC Cyber Security Plan (the Plan), an Implementation Schedule, and a proposed sentence to be added to the existing Facility Operating License (FOL) Physical Protection license condition for Unit 1 and Unit 2.

### **2. DETAILED DESCRIPTION**

The proposed license amendment request includes three parts: the proposed Plan, an Implementation Schedule, and a proposed sentence to be added to the existing FOL Physical Protection license condition to require PPL Susquehanna to fully implement and maintain in effect all provisions of the Commission approved cyber security plan as required by 10 CFR §73.54. *Federal Register* notice issued the final rule that amended 10 CFR Part 73. The regulations in 10 CFR §73.54, "Protection of digital computer and communication systems and networks," 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 NRC Notice of Availability published on March 27, 2009, 74 FR 13926 (Reference 1).

### **3. TECHNICAL EVALUATION**

*Federal Register* notice 74 FR 13926 issued the final rule that amended 10 CFR Part 73. Cyber security requirements are codified as new §73.54 and are designed to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks up to and including the design basis threat established by § 73.1(a)(1)(v). These requirements are substantial improvements upon the requirements imposed by EA-02-026 (Reference 2).

NRC issued pre-decisional Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities" which provides an approach the NRC staff deems acceptable for complying with the Commission's regulations for protecting digital computers, communications systems, and networks. NEI 08-09, "Cyber Security Plan Template" has been developed by NEI (Reference 3) for use by licensees in development of their own cyber security plans.

This license amendment request includes the proposed Cyber Security Plan (Enclosure 3) that conforms to the template provided in NEI 08-09, Revision 6 with the exception of the definition of "cyber attack" that has been modified to align with agreements reached with the NRC staff. In addition, the license amendment request includes the proposed change to the existing Unit 1 and Unit 2 FOL license condition for "Physical Protection" (Enclosure 1, Attachments 1 and 2). Finally, the license amendment request contains the proposed Implementation Schedule (Enclosure 2) as required by 10 CFR §73.54.

#### **4. REGULATORY EVALUATION**

##### **4.1 Applicable Regulatory Requirements / Criteria**

This license amendment request is submitted pursuant to 10 CFR §73.54 which requires licensees currently licensed to operate a nuclear power plant under 10 CFR Part 50 to submit a Cyber Security Plan as specified in §50.4 and §50.90.

##### **4.2 Significant Hazards Consideration**

PPL has evaluated the proposed changes using the criteria in 10 CFR 50.92 and has determined that the proposed changes do not involve a significant hazards consideration. An analysis of the issue of no significant hazards consideration is presented below.

The proposed license amendment request includes three parts: the proposed PPL Susquehanna, LLC Cyber Security Plan, an Implementation Schedule, and a proposed sentence to be added to the existing Facility Operating License (FOL) Physical Protection license condition to require PPL Susquehanna Units 1 and 2 to fully implement and maintain in effect all provisions of the Commission-approved cyber security plan as required by 10 CFR §73.54. The regulations in 10 CFR §73.54, "Protection of digital computer and communication systems and networks," establish the requirements for a cyber security program.

The Cyber Security Plan conforms to the template provided in NEI 08-09, Revision 6, with the exception that the definition of "cyber attacks" has been modified to align with agreements reached with the NRC staff. The plan also provides a description of how the

requirements of 10 CFR §73.54 will be implemented at PPL Susquehanna Units 1 and 2 in order to protect the health and safety of the public from radiological sabotage as a result of a cyber attack. The Cyber Security Plan establishes the licensing basis for the PPL Cyber Security Program for Susquehanna Units 1 and 2. The Cyber Security Plan establishes how to achieve high assurance that nuclear power plant digital computer and communication systems and networks associated with the following are adequately protected against cyber attacks up to and including the design basis threat:

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 safety, security, or emergency preparedness functions.

**(1) *Does the proposed amendment involve a significant increase in the probability or consequences of an accident previously evaluated?***

Response: No.

The proposed amendment incorporates a new requirement in the PPL Susquehanna Units 1 and 2 FOL to implement and maintain a Cyber Security Plan as part of the facility's overall program for physical protection. Inclusion of the Cyber Security Plan in the FOL itself does not involve any modifications to the safety-related structures, systems or components (SSCs). Rather, the Cyber Security Plan describes how the requirements of 10 CFR 73.54 are to be implemented to identify, evaluate, and mitigate cyber attacks up to and including the design basis cyber attack threat, thereby achieving high assurance that the facility's digital computer and communications systems and networks are protected from cyber attacks. The Cyber Security Plan will not alter previously evaluated Final Safety Analysis Report (FSAR) design basis accident analysis assumptions, add any accident initiators, or affect the function of the plant safety-related SSCs as to how they are operated, maintained, modified, tested, or inspected. Therefore, the proposed amendment does not involve a significant increase in the probability or consequences of an accident previously evaluated.

**(2) *Does the proposed amendment create the possibility of a new or different kind of accident from any accident previously evaluated?***

Response: No.

This proposed amendment provides assurance that safety-related SSCs are protected from cyber attacks. Implementation of 10 CFR 73.54 and the inclusion

of a plan in the PPL Susquehanna Units 1 and 2 FOL do not result in the need for any new or different FSAR design basis accident analysis. The inclusion does not introduce new equipment that could create a new or different kind of accident, and no new equipment failure modes are created. The inclusion of the Cyber Security Plan also does not affect the function of any safety-related SSC as to how they are operated, maintained, modified, tested or inspected. As a result, no new accident scenarios, failure mechanisms, or limiting single failures are introduced as a result of this proposed amendment. Therefore, the proposed amendment does not create a possibility for an accident of a new or different type than those previously evaluated.

**(3) *Does the proposed amendment involve a significant reduction in a margin of safety?***

Response: No.

The margin of safety is associated with the confidence in the ability of the fission product barriers (i.e., fuel cladding, reactor coolant pressure boundary, and containment structure) to limit the level of radiation to the public. The proposed amendment would not alter the way safety-related SSCs function and would not alter the way PPL Susquehanna Units 1 and 2 are operated. The amendment provides assurance that safety-related SSCs are protected from cyber attacks. The proposed amendment would not introduce any new uncertainties or change any existing uncertainties associated with the design basis or any safety limit. The proposed amendment would have no impact on the structural integrity of the fuel cladding, reactor coolant pressure boundary, or containment structure. Based on the above considerations, the proposed amendment would not degrade the confidence in the ability of the fission product barriers to limit the level of radiation to the public. Therefore, the proposed change does not involve a significant reduction in a margin of safety.

### **4.3 Conclusion**

In conclusion, based on the considerations discussed above: (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.



**5. ENVIRONMENTAL CONSIDERATION**

The proposed amendment establishes the licensing basis for a Cyber Security Program for PPL Susquehanna, Units 1 and 2 and will be a part of the Physical Security Plan. This proposed amendment will not involve any significant construction impacts. Pursuant to 10 CFR 51.22(b)(12) no environmental impact statement or environmental assessment need be prepared in connection with the issuance of the amendment.

**6. REFERENCES**

1. Federal Register Notice, Final Rule 10 CFR Part 73, Power Reactor Security Requirements, published on March 27, 2009, 74 FR 13926.
2. EA-02-026, Order Modifying Licenses, Safeguards and Security Plan Requirements, issued February 25, 2002.
3. NEI 08-09, Revision 6, Cyber Security Plan for Nuclear Power Reactors.

**Attachment 1 to Enclosure 1**

**Facility Operating License, PPL Susquehanna  
Unit 1 Mark-Up**

(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.

PPL shall fully implement and maintain in effect all provisions of the Commission-approved PPL Cyber Security Plan submitted in PLA-6628 and withheld from public disclosure in accordance with 10CFR 2.390.

**Attachment 2 to Enclosure 1**

**Facility Operating License, PPL Susquehanna  
Unit 2 Mark-Up**

(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.

PPL shall fully implement and maintain in effect all provisions of the Commission-approved PPL Cyber Security Plan submitted in PLA-6628 and withheld from public disclosure in accordance with 10CFR 2.390.

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.

---

**Enclosure 2 to PLA-6628**

**PPL Susquehanna, LLC**

**Cyber Security Plan**

**Implementation Schedule**

---

## PPL SUSQUEHANNA, LLC

---

### **Cyber Security Plan Implementation Schedule**

Generic RAI Question # 29 includes reference to previous regulatory guidance and industry initiatives related to cyber security. As referenced, current industry guidance for cyber security is described in NEI 04-04, *Cyber Security Program for Power Reactors*. However, the scope of requirements in the NRC accepted implementation guidance contained in NEI 08-09 revision 6 are significantly greater than the previously implemented cyber security program. The defensive model design requirements, the new digital asset assessment methodology and the resultant digital asset remediation actions will require a significant expenditure of labor resources. As referenced in the Generic RAI Question # 29, PPL Susquehanna, LLC is also required to implement a separate cyber security program in accordance with the NERC Critical Infrastructure Protection Standards. While the timeframe for implementation is shorter for the NERC regulation as described in the RAI question, the NERC cyber security methodology is different from the NRC Rule requirements. The NERC requirements are based on a logical risk based assessment process while the NRC Rule 73.54 requires a deterministic cyber security assessment methodology.

In light of the extensive work associated with implementation of these two new regulations, PPL Susquehanna, LLC has developed a prioritized approach to establish the NRC Rule 73.54 implementation schedule. PPL Susquehanna, LLC realizes the importance of deploying a boundary control communication barrier to protect the most critical SSEP functions. One major activity is the deployment of boundary control communication barrier to ensure protection from remote attacks on plant systems. While the deployment of the boundary control barrier is critical to protection from external cyber threats, it also impacts remote access to plant data systems by authorized personnel. This elimination of remote access will require Licensees to develop and implement a detailed change management plan.

Another major activity is the performance of individual critical digital asset (CDA) assessments to identify individual asset security control remediation actions. Programs and procedures are being developed to implement the programmatic requirements of the regulation. The cyber security assessment teams are also being established for execution of program requirements. These teams are required to have extensive knowledge of plant systems and cyber security control technology. A comprehensive training program will be required to ensure competent personnel for program execution.

Following are the Cyber Security implementation milestones that have been developed based on the sample listing of milestones provided with the NRC December 2009 implementation schedule guidance:

## PPL SUSQUEHANNA, LLC

Implementation Milestone	Completion Date	Basis
Train and Qualify Cyber Security Assessment Team (CSAT)	6/30/2011	<p>The CSAT will require a broad and very specialized knowledge of information and digital systems technology. The CSAT will need to have digital plant systems knowledge as well as nuclear power plant operations, engineering and nuclear safety experience and technical expertise. The personnel selected for this team will require additional training in these areas to ensure adequate capabilities to meet the regulation requirements.</p> <p>By the completion date, the following will be performed:</p> <ul style="list-style-type: none"> <li>• Cyber security assessment procedures/tools will be developed and available; includes tools specification and development, and approved procedures described in the approved Plan.</li> <li>• Qualifications for CSAT will be developed; and</li> <li>• Training of the CSAT will be completed.</li> </ul>
Identify Critical Systems (CSs) and Critical Digital Assets (CDAs)	6/30/2011	<p>By the completion date, the following will be performed:</p> <ul style="list-style-type: none"> <li>• Critical Systems will be identified; and</li> <li>• Critical Digital Assets will be identified.</li> </ul>
Develop Cyber Security Defensive Strategy (i.e., defensive model)	6/30/2011	<p>The Defensive Strategy expands upon the high level model in the Cyber Security Plan and requires assessment of existing site and corporate policies, comparison to new requirements, revisions as required, and communication to plant personnel.</p> <p>By the completion date, the following will be performed:</p> <ul style="list-style-type: none"> <li>• Documenting the defense-in-depth architecture and defensive strategy;</li> <li>• Revisions to existing defensive strategy policies will be implemented and communicated; and</li> <li>• Planning the implementation of the defense-in-depth architecture.</li> </ul>
Implement cyber security defense-in-depth architecture	6/30/2012 for deterministic isolation devices. 6/30/2013 for other boundary control devices	<p>The implementation of communication barriers protects the most critical SSEP functions from remote attacks on our plant systems. 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 and other plant staff. This elimination of remote access to core monitoring systems requires the development and execution of a detailed change management plan to ensure continued safe operation of the plants.</p>



## PPL SUSQUEHANNA, LLC

Implementation Milestone	Completion Date	Basis
		<p>Vendors may be required to develop software revisions to support the model. The modification will be developed, prioritized and scheduled. Since software must be updated on and data retrieved from isolated systems, a method of patching, updating and scanning isolated devices will be developed.</p> <p>By the completion date, the following will be performed:</p> <ul style="list-style-type: none"> <li>• Installation of boundary layer control devices to implement defensive layer boundaries.</li> </ul>
Establish Cyber Security Program policies/procedures	12/31/2013	<p>The implementation of the cyber security program is expected to require policy/procedure development and/or upgrades for nearly every plant department. The procedural development for the cyber security program requirements and all of the individual security controls will be far-reaching. Many of the security controls will require development of the technical processes for implementing the control in a nuclear plant environment including development of new procedures for surveillances, periodic monitoring and reviews. Procedure development will begin early in the implementation of the program and continue until the specified completion date.</p> <p>By the completion date, the following will be performed:</p> <ul style="list-style-type: none"> <li>• Policies/procedures will be updated to establish Cyber Security Program ;</li> <li>• The Cyber Security Assessment Procedure will be issued; and</li> <li>• New policies/procedures or revision of existing policies/procedures in areas impacted by cyber security requirements will be develop and implemented.</li> </ul>
Perform and document the cyber security assessment described in the Cyber Security Plan	12/31/2013	<p>Based on the existing cyber security program, it is known that the number of digital assets requiring assessment is extensive. As previously discussed, the CDA assessment methodology required for this regulation is extremely rigorous and deterministic. The completion of these assessments will require a significant commitment of resources. The assessments will not begin prior to having a fully established CSAT and the required procedures.</p> <p>Performing the assessments will require participation of multiple disciplines and involve document reviews, system configuration evaluation, physical walk downs or electronic verification of every communication pathway for each CDA, and documentation of results. These tasks will need to be</p>

PPL SUSQUEHANNA, LLC

Implementation Milestone	Completion Date	Basis
		<p>coordinated and scheduled to align with department resource availability and system access requirements.</p> <p>By the completion date, the following will be performed:</p> <ul style="list-style-type: none"> <li>• Cyber security assessments will be performed and documented.</li> </ul>
<p>Implement Security Controls (outage and non-outage)</p>	<p>12/01/2014 for changes not requiring an Engineering Change. 12/01/2015 for changes requiring an Engineering Change.</p>	<p>Although the scope of individual CDA assessment remediation actions is unknown, based on the number and complexity of the required security controls, it is expected to be a significant effort. Each of the individual CDA remediation actions will need to be planned, resourced, and executed. A rigorous planning process is used to ensure safe execution of refueling outage and non-outage work. The potential system modifications required by this regulation need to be carefully planned and executed to ensure no detrimental effect to safe plant operations.</p>
<p>The Cyber Program is implemented and the Program has entered the maintenance phase</p>	<p>12/01/2015</p>	<p>By the completion date, the following will be performed:</p> <ul style="list-style-type: none"> <li>• Security controls will be implemented in accordance with Section 3.1.6 of the Plan.</li> </ul> <p>Beginning on this date, during the ongoing maintenance of the Program, the requirements of Section 4 of the Plan will be effective</p>