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

APR 0 4 2011

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

SUSQUEHANNA STEAM ELECTRIC STATION
RESPONSE TO CYBER SECURITY REQUEST FOR
ADDITIONAL INFORMATION **Docket Nos. 50-387**
PLA-6704 **and 50-388**

References: 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: Withdrawal and Resubmittal of Request for Approval of the PPL Susquehanna, LLC Cyber Security Plan," dated July 22, 2010.

2) Letter from NRC (Bhalchandra K. Vaidya) to PPL (Mr. Timothy S. Rausch), "Susquehanna Steam Electric Station, Units 1 and 2 - Request for Additional Information Regarding Amendment Application for Approval of the Susquehanna Steam Electric Station, Units 1 And 2 Cyber Security Plan (TAC Nos. ME4420 and ME4421), dated March 3, 2011.

In Reference 1, PPL Susquehanna, LLC (PPL) submitted requests for amendments to the Facility Operating Licenses (FOL) for the Susquehanna Steam Electric Station, Units 1 and 2. The proposed amendments requested NRC approval of the PPL Cyber Security Plan, revisions to the existing FOL Physical Protection license condition, and the Cyber Security Plan implementation schedule.

In Reference 2, the NRC requested additional information regarding the PPL Cyber Security Plan and the associated implementation schedule.

Enclosure 1 to this letter provides the PPL response to the NRC request for additional information. A revised implementation schedule is included in Enclosure 2. Enclosure 3 provides a revised copy of the PPL Susquehanna, LLC Cyber Security Plan, which incorporates changes based on the RAI response. PPL requests that Enclosure 3, which contains security-related information, be withheld from public disclosure in accordance with 10 CFR 2.390.

The enclosed implementation schedule and Cyber Security Plan replace, in their entirety, the schedule and plan previously submitted in Reference 1.

SOOIA
NRR

The changes do not affect the conclusions of the no significant hazards consideration determination previously provided in Reference 1.

The implementation schedule includes actions that are considered regulatory commitments. These commitments supersede and replace the commitments made in Reference 1.

If you should have any questions regarding this submittal, please contact Mr. John Petrilla at (570) 542-3796.

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

Executed on: 4/4/2011

T. S. Rausch

Enclosures:

1. Response to NRC Request for Additional Information Regarding the PPL Cyber Security Plan
2. Revised Implementation Schedule Associated with the PPL Cyber Security Plan
3. PPL Susquehanna, LLC Cyber Security Plan [Security-Related Information – Withhold Under 10 CFR 2.390]

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

Enclosure 1 to PLA-6704

Response to NRC Request for Additional Information Regarding the PPL Cyber Security Plan

Response to NRC Request for Additional Information

On March 3, 2011, the NRC issued a request for additional information (RAI) to PPL Susquehanna, LLC (PPL) regarding the PPL Cyber Security Plan and associated implementation schedule. PPL's response to the RAI is provided below.

RAI 1: Records Retention

NRC Question:

"Title 10 of the Code of Federal Regulations (10 CFR) Paragraph 73.54(c)(2) requires licensees to design a cyber security program to ensure the capability to detect, respond to, and recover from cyber attacks. Furthermore, 10 CFR 73.54(e)(2)(i) requires licensees to maintain a cyber security plan that describes how the licensee will maintain the capability for timely detection and response to cyber attacks. The ability for a licensee to detect and respond to cyber attacks requires accurate and complete records and is further supported by 10 CFR 73.54(h), which states that the licensee shall retain all records and supporting technical documentation required to satisfy the requirements of 10 CFR Section 73.54 as a record until the Commission terminates the license for which the records were developed, and shall maintain superseded portions of these records for at least 3 years after the record is superseded, unless otherwise specified by the Commission.

The licensee's Cyber Security Plan (CSP) in Section [4.13] states that Critical Digital Asset (CDA) audit records and audit data (e.g., operating system logs, network device logs) are retained for a period of time that is less than what is required by 10 CFR 73.54(h).

Explain the deviation from the 10 CFR 73.54(h) requirement to retain records and supporting technical documentation until the Commission terminates the license (or to maintain superseded portions of these records for at least 3 years) and how that meets the requirements of 10 CFR 73.54."

PPL Response:

The PPL Cyber Security plan has been updated to require that records be retained until the Commission terminates the license and that superseded portions of these records be retained for at least 3 years after the record is superseded. This update is consistent with the wording provided in a letter from Christopher E. Earls (NEI) to Mr. Richard P. Correia (NRC) dated February 28, 2011 and accepted by the NRC in a letter from Richard P. Correia to Mr. Christopher E. Earls dated March 1, 2011. The revised PPL Cyber Security Plan is included as Enclosure 3.

RAI 2: Implementation Schedule

NRC Question:

"The regulation at 10 CFR 73.54, "Protection of digital computer and communication systems and networks," requires licensees to submit a CSP that satisfies the requirements of this section for Commission review and approval. Furthermore, each submittal must include a proposed implementation schedule and the implementation of the licensee's cyber security program must be consistent with the approved schedule. Paragraph 73.54(a) of 10 CFR requires licensees 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.

The completion of several key intermediate milestones (Items (a) through (g) below) would demonstrate progress toward meeting the requirements of 10 CFR 73.54. The Nuclear Regulatory Commission (NRC) staff's expectation is that the key intermediate milestones will be completed in a timely manner, but no later than December 31, 2012. The key CSP implementation milestones are as follows:

(a) Establish, train and qualify Cyber Security Assessment Team, as described in Section 3.1.2, "Cyber Security Assessment Team," of the CSP.

(b) Identify Critical Systems and CDAs, as described in Section 3.1.3, "Identification of Critical Digital Assets," of the CSP.

(c) Implement cyber security defense-in-depth architecture by installation of [deterministic one-way] devices, as described in Section 4.3, "Defense-In-Depth Protective Strategies" of the CSP.

(d) Implement the management, operational and technical cyber security controls that address attacks promulgated by use of portable media, portable devices, and portable equipment as described in Appendix D Section 1.19 "Access Control for Portable and Mobile Devices," of Nuclear Energy Institute (NEI) 08-09, Revision 6.

(e) Implement observation and identification of obvious cyber related tampering to existing insider mitigation rounds as described in Appendix E Section 4.3, "Personnel Performing Maintenance and Testing Activities," and Appendix E Section 10.3, "Baseline Configuration" of NEI 08-09, Revision 6.

(f) Identify, document, and implement cyber security controls to physical security target set CDAs in accordance with Section 3.1.6, "Mitigation of Vulnerabilities and Application of Cyber Security Controls," of the CSP.

(g) Ongoing monitoring and assessment activities will commence for those target set CDAs whose security controls have been implemented, as described in Section 4.4, "Ongoing Monitoring and Assessment," of the CSP

(h) Full implementation of the CSP for all safety, security, and emergency preparedness functions.

Provide a revised CSP implementation schedule that identifies the appropriate milestones, completion dates, supporting rationale, and level of detail to allow the NRC to evaluate the licensee's proposed schedule and associated milestone dates, which include the final completion date. It is the NRC's intention to develop a license condition incorporating your revised CSP implementation schedule containing the key milestone dates."

PPL Response:

PPL's revised implementation schedule is included as Enclosure 2 to this submittal. The revised schedule includes the key milestones and indicates that Milestones 1 – 7 will be completed no later than 12/31/2011 and that full implementation will be completed by 12/1/2015. The schedule is consistent with the template provided in a letter from Christopher E. Earls (NEI) to Mr. Richard P. Correia (NRC) dated February 28, 2011 and accepted by the NRC in a letter from Richard P. Correia to Mr. Christopher E. Earls dated March 1, 2011 except for a minor change to the black text for Milestone 3. The second sentence of the template for Milestone 3 states the following:

"Lower security level devices ([level 0, 1, 2 devices]) that bypass the deterministic device and connect to level 3 or 4 will be modified to prevent the digital connectivity to the higher level or will be modified to meet cyber security requirements commensurate with the level [3 or 4] devices to which they connect."

The change involves deletion of the "3 or". The proposed PPL wording is as follows:

Lower security level devices (level 0, 1, 2, 3 devices) that bypass the deterministic device and connect to level 4 will be modified to prevent the digital connectivity to the higher level or will be modified to meet cyber security requirements commensurate with the level 4 devices to which they connect.

This change is intended to align the wording in the implementation schedule with the defensive strategy described in the PPL Cyber Security Plan.

RAI 3: Scope of Systems

NRC Question:

"Paragraph 73.54(a) of 10 CFR requires licensees 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 as described in 10 CFR 73.1. In addition, 10 CFR 73.54(a)(1) states that 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 functions.

Subsequent to the issuance of the cyber security rule, the NRC stated that 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 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML103490344, dated November 19, 2010). The SSCs in the BOP are those that could directly or indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient and are therefore, within the scope of important-to-safety functions described in 10 CFR 73.54(a)(1). Furthermore, the NRC issued a letter to NEI dated January 5, 2011 (ADAMS Accession No. ML103550480) that provided licensees with additional guidance on one acceptable approach to comply with the Commission's policy determination.

Explain how the scoping of systems provided by [site/licensee]'s CSP meets the requirements of 10 CFR 73.54 and the additional guidance provided by the NRC."

PPL Response:

Wording consistent with the January 5, 2011 letter has been added to PPL's Cyber Security Plan under Section 2.1. The revised PPL Cyber Security Plan is included as Enclosure 3.

Enclosure 2 to PLA-6704

Revised Implementation Schedule Associated with the PPL Cyber Security Plan

Cyber Security Plan Implementation Schedule

Full implementation of the cyber security program involves many supporting tasks. Major activities include: program and procedure development; performing of individual critical digital asset (CDA) assessments; and identification, scheduling, and implementing individual asset security control design remediation actions through the site configuration management program. These design modifications may be performed on-line or could require a refueling outage for installation.

The extensive workload associated with full implementation of the Cyber Security Plan (CSP) requires prioritization to assure those activities that provide higher degrees of protection against radiological sabotage are performed first. Therefore the CSP implementation schedule will be implemented with two major milestone dates. The first milestone date of no later than December 31, 2012, includes the activities listed in the table below. The second milestone date, December 1, 2015, includes the completion of all remaining actions that result in the full implementation of the cyber security plan for all applicable Safety, Security, and Emergency Preparedness (SSEP) functions. This date also bounds the completion of all individual asset security control design remediation actions.

Cyber security controls are not applied if the control adversely impacts safety and important to safety, security or emergency preparedness functions.

#	Implementation Milestone	Completion Date	Basis
1	Establish Cyber Security Assessment Team (CSAT) as described in Section 3.1.2 "Cyber Security Assessment Team" of the Cyber Security Plan (CSP).	No later than December 31, 2012	The CSAT, collectively, 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 may require additional training in these areas help to ensure adequate capabilities to perform cyber security assessments as well as others duties.
2	Identify Critical Systems (CSs) and Critical Digital Assets (CDAs) as described in Section 3.1.3 "Identification of Critical Digital Assets" of the CSP.	No later than December 31, 2012	The scope of 10 CFR 73.54 includes digital computer and communication systems and networks associated with: safety-related and important-to safety functions; security functions; emergency preparedness functions, including offsite communications; and support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions. The scope of 10 CFR 73.54 includes structures, systems, and components (SSCs) that have a nexus to radiological health and safety and therefore can directly or indirectly affect reactivity of a nuclear power plant and could

#	Implementation Milestone	Completion Date	Basis
			result in an unplanned reactor shutdown or transient.
3	Implement Installation of a deterministic one-way device between lower level devices (level 0 1,2,3) and the higher level devices (level 4 Safety and Security) as described in Section 4.3, "Defense-In-Depth Protective Strategies" of the CSP. Lower security level devices (level 0, 1, 2,3 devices) that bypass the deterministic device and connect to level 4 will be modified to prevent the digital connectivity to the higher level or will be modified to meet cyber security requirements commensurate with the level 4 devices to which they connect. The design modifications that are not finished by the completion date will be documented in the site configuration management and/or change control program to assure completion of the design modification as soon as possible, but no later than the final implementation date.	No later than December 31, 2012	The implementation of communication barriers protects the most critical SSEP functions from remote attacks on plant systems. Isolating the plant systems from the internet as well as from the corporate business systems is an important milestone in defending against external threats. While the deployment of the barriers is critical to protection from external cyber threats, it also prevents remote access to core monitoring and plant data systems for reactor engineers, plant operations, and other plant staff. This elimination of remote access to reactor core monitoring systems may require the development and execution of a detailed change management plan to ensure continued safe operation of the plants. Vendors may be required to develop software revisions to support the model. The modification will be developed, prioritized and scheduled.
4	The security control "Access Control For Portable And Mobile Devices" described in Appendix D 1.19 of NEI 08-09, Revision 6, will be implemented.	No later than December 31, 2012	Portable media devices are used to transfer electronic information (e.g., data, software, firmware, virus engine updates and configuration information) to and from plant process equipment. Careful use of this class of media is required to minimize the spread of malicious software to plant process equipment. The effective implementation of this control may require the coordinated implementation of other complimentary controls to ensure adequate mitigation.
5	Implement observation and identification of obvious cyber related tampering to existing insider mitigation	No later than December 31, 2012	Insider mitigation rounds by trained staff look for obvious signs of cyber related tampering and would provide mitigation of observable cyber

#	Implementation Milestone	Completion Date	Basis
	rounds by incorporating the appropriate elements in Appendix E Section 4.3 "Personnel Performing Maintenance And Testing Activities."		related insider actions. Implementing steps to add signs of cyber security-related tampering to insider mitigation rounds will be performed by the completion date.
6	Identify, document, and implement cyber security controls in accordance with the Cyber Security Plan Section 3.1.6 "Mitigation of Vulnerabilities and Application of Cyber Security Controls" for CDAs that could adversely impact the design function of physical security target set equipment. The implementation of controls that require a design modification that are not finished by the completion date will be documented in the site configuration management and/or change control program to assure completion of the design modification as soon as possible, but no later than the final implementation date.	No later than December 31, 2012	The site physical protection program provides high assurance that these elements are protected from physical harm by an adversary. The cyber security program will enhance the defense-in-depth nature of the protection of CDAs associated with target sets. Implementing Cyber Security Plan security controls to target set CDAs provides a high degree of protection against a cyber related attacks that could lead to radiological sabotage. Security controls will be addressed in accordance with Cyber Security Plan Section 3.1.6 with the exception of those that require a design modification.
7	Ongoing monitoring and assessment activities commence, as described in Section 4.4, "Ongoing Monitoring and Assessment" of the CSP, for those target set CDAs whose security controls have been implemented.	No later than December 31, 2012	The ongoing monitoring and assessment activities as described in Section 4.4, "Ongoing Monitoring and Assessment" of the Cyber Security Plan will be implemented for the controls applied to target set CDAs. This action results in the commencement of the cyber security program for target set related CDAs.
8	Full implementation of the PPL Susquehanna, LLC Cyber Security Plan for all SSEP functions will be achieved.	December 1, 2015	By the completion date, the PPL Susquehanna, LLC Cyber Security Plan will be fully implemented for all SSEP functions in accordance with 10 CFR 73.54. This date also bounds the completion of all individual asset security control design remediation actions including those that require a refuel outage for implementation.