



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

March 3, 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 - 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)

Dear Mr. Rausch:

By letter dated July 22, 2010 (Agencywide Documents Access and Management System, Accession No. ML102150151), as supplemented by letter dated September 29, 2010, (ADAMS Accession Nos. ML102720947), PPL Susquehanna, LLC (the licensee) resubmitted a request to amend the Facility Operating Licenses (Nos. NPF-14 and NPF-22) for Susquehanna Steam Electric Station, Units 1 and 2 (SSES 1 & 2). The licensee requested approval of the SSES 1 & 2 Cyber Security Plan (CSP) (ML102150152), provided a proposed CSP Implementation Schedule, and included a proposed revision to the Facility Operating License to incorporate the provisions for implementing and maintaining in effect the provisions of the approved CSP. The licensee's amendment request was based on a generic template developed by the Nuclear Energy Institute (NEI) in concert with the industry.

The U.S. Nuclear Regulatory Commission (NRC) staff is reviewing the CSP and the proposed CSP Implementation Schedule and has determined that additional information is required to complete its technical review. The specific questions are found in the enclosed request for additional information (RAI).

It is our understanding that the NEI and the industry Cyber Security Task Force are working to ensure that operating reactor licensees will submit consistent responses to these generic RAIs to the NRC. Through the NEI working group, licensees have been aware of these three generic questions for several months and should have been framing out their responses to these expected questions in advance of receiving RAI's from the staff. The NRC staff has sent the letters to NEI on February 28, 2011, indicating that the NRC staff has no issues with respect to the template responses addressing the RAIs related to Records Retention and Implementation Schedule. NEI has indicated that it has received the correspondence from the NRC on March 1, 2011. Therefore, the NRC staff believes that a 30-day response time should be more than adequate under these circumstances.

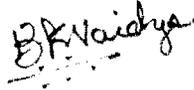
T. S. Rausch

- 2 -

Please provide the supplemental submission with the responses to the enclosed RAIs within 30 days from the date of this letter.

Please contact me at (301) 415-3308 if you have any questions.

Sincerely,

Handwritten signature of Bhalchandra K. Vaidya in black ink.

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

Enclosure:
As stated

cc w/encl: Distribution via Listserv

REQUEST FOR ADDITIONAL INFORMATION (RAI)

REGARDING LICENSE AMENDMENT REQUEST FOR THE CYBER SECURITY PLAN

PPL SUSQUEHANNA, LLC

ALLEGHENY ELECTRIC COOPERATIVE, INC.

SUSQUEHANNA STEAM ELECTRIC STATION, UNITS 1 AND 2

DOCKET NOS. 50-387 AND 388

RAI 1: Records Retention

Title 10 of the *Code of Federal Regulations* (10 CFR) Section 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 (CSP) 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 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 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.

RAI 2: Implementation Schedule

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. 10 CFR 73.54(a) 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 (DBT). 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

Enclosure

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.

RAI 3: Scope of Systems

10 CFR 73.54(a) 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 DBT 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 licensee's CSP meets the requirements of 10 CFR 73.54 and the additional guidance provided by the NRC.

T. S. Rausch

- 2 -

Please provide the supplemental submission with the responses to the enclosed RAIs within 30 days from the date of this letter.

Please contact me at (301) 415-3308 if you have any questions.

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

Enclosure:
As stated

cc w/encl: Distribution via Listserv

DISTRIBUTION:

PUBLIC LPL1-1 R/F RidsNRRDorILPI1-1 RidsNRRPMSusquehanna
RidsNrrLASLittle (hard copy) RidsOGCMailCenter RidsNsirDsplscpb
RidsNrrDorIDpr RidsNrrDirsltsb RidsAcrcAcnw&mMailCenter
RidsRg1MailCenter PKrohn, RI R. Pascarelli, NRR/DORL
C. Erlanger, NSIR/ISCPB P. Pederson, NSIR/ISCPB
B. Singal, NRR/DORL T. Wengert, NRR/DORL

ADAMS Accession No.: ML11060A027

(*) – No substantial change in the RAI Memo

OFFICE	LPL1-1/PM	LPL1-1/LA	NSIR/DSP/ISCPB/BC(*)	LPL1-1/BC	LPL1-1/PM
NAME	BVaidya	SLittle	CErlanger	NSalgado	BVaidya
DATE	03/03/11	03/03/11	02/18/11	03/03/11	03/03/11

OFFICIAL RECORD COPY