OFFICE OF NUCLEAR SECURITY AND INCIDENT RESPONSE

REQUEST FOR ADDITIONAL INFORMATION

CHANGES TO CYBER SECURITY IMPLEMENTATION SCHEDULE

MILESTONES 3 AND 6

PPL SUSQUEHANNA, LLC

ALLEGHANY ELECTRIC COOPERATION, INC.

SUSQUEHANNA STEAM ELECTRIC STATION, UNITS 1 AND 2

DOCKET NUMBERS 50-387 AND 50-388

By letter dated April 30, 2012,[1] PPL Susquehanna, LLC (PPL) submitted a license amendment request for Susquehanna Steam Electric Station, Units 1 and 2 (SSES). The proposed amendment would make changes to the Cyber Security Implementation Schedule for Milestone 3 and 6. Specifically, for Milestone 3, PPL proposes to install a deterministic data diode appliance between Layers 3 and 2 instead of between Layers 3 and 4, with no change to the approved implementation date. For Milestone 6, PPL proposes to implement the technical controls for critical digital assets (CDAs) that could adversely impact the design function of physical security target set equipment by the approved implementation date, and to implement the operational and management controls for CDAs in conjunction with the full implementation of the Cyber Security Program.

The U.S. Nuclear Regulatory Commission (NRC) staff has reviewed the information provided by the licensee and has determined that the following additional information is needed in order to complete the review.

Milestone 3 of the Cyber Security Implementation Schedule implements installation of a deterministic one-way device between lower-level devices and higher-level devices as described in Section 4.3, "Defense-in-Depth Protective Strategies" of the Cyber Security Plan (CSP). In the April 30, 2012, request, PPL states that (emphasis added) "[f]or *non-security critical digital assets* (CDAs), the current implementation schedule and cyber security plan describe deterministic devices between Layers 3 and 4 with firewalls between Layers 1 and 2 and between Layers 2 and 3." PPL goes on to describe that the proposed change to the cyber defensive strategy would install a deterministic device between Layers 2 and 3 with firewalls between the other layers.

1. Please clarify that this proposed change not only impacts Milestone 3, but also directly impacts the CSP, Section 4.3, "Defense-in-Depth Protective Strategies."

In the approved CSP, safety and security CDAs were isolated from all other CDAs through the use of deterministic boundary devices (i.e., data diodes, air gaps, etc.) between Levels 4 and 3;

---

[1] Agencywide Documents Access and Management System (ADAMS) Accession No. ML12122A011

information flows between Level 3 and 2 and between Level 2 and 1 were restricted through the use of a firewall and network-based intrusion detection system.

In the proposed LAR, for security CDAs, the boundary between Level 4 and 3 will be implemented by one or more deterministic devices; information flows between Level 3 and lower levels are restricted through the use of firewalls and network-based intrusion detection system(s). For non-security CDAs, the boundary between Level 3 and 2 will be implemented by one or more deterministic devices and information flows between Level 3 and 4 and between Level 2 and 1 are restricted through the use of firewall(s) and network-based intrusion detection system(s).

2. Please explain how the proposed changes to the defensive architecture will provide the same level of protection as the current, approved defensive architecture described above.

In the approved defensive architecture section, a description of communications between safety and non-safety systems within Level 4 was not necessary because they were both isolated from lower levels by a deterministic device (i.e., diode). For the proposed defensive architecture, a detailed description of communication within Level 4 and Level 3 are critical to determine whether or not the proposed changes will provide similar security as the existing architecture.

3. Please provide the detailed description of communication within Level 4 and Level 3 of the proposed defensive architecture described above.