



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

March 8, 2011

Mr. Mano Nazar  
Executive Vice President and  
Chief Nuclear Officer  
Florida Power and Light Company  
P.O. Box 14000  
Juno Beach, Florida 33408-0420

SUBJECT: TURKEY POINT UNITS 3 AND 4 - REQUEST FOR ADDITIONAL  
INFORMATION REGARDING AMENDMENT APPLICATION FOR APPROVAL  
OF THE CYBER SECURITY PLAN (TAC NOS. ME4549 AND ME4550)

Dear Mr. Nazar:

By letter dated July 28, 2010, Florida Power & Light Company submitted a license amendment for Turkey Point, Units 3 and 4. The proposed amendment would establish a Cyber Security Plan in conformance with Nuclear Energy Institute (NEI) document NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6, dated April 2010, with three deviations regarding the definition of a Cyber Attack, Emergency Preparedness, and the Turkey Point equivalency of the Senior Nuclear Management as defined in NEI 08-09, Revision 6.

The Nuclear Regulatory Commission (NRC) staff is reviewing the submittal and has determined that additional information is needed to complete its review. The specific questions are found in the enclosed request for additional information (RAI). The NRC staff is requesting a response to the RAI within 30 days of receipt.

If you have any questions regarding this issue, please contact me at (301) 415-5888.

Sincerely,

A handwritten signature in black ink, appearing to read "Jason C. Paige".

Jason C. Paige, Project Manager  
Plant Licensing Branch II-2  
Division of Operating Reactor Licensing  
Office of Nuclear Reactor Regulation

Docket Nos. 50-250 and 50-251

Enclosure:  
Request for Additional Information

cc w/encl: Distribution via Listserv

REQUEST FOR ADDITIONAL INFORMATION

REGARDING LICENSE AMENDMENT REQUEST FOR THE CYBER SECURITY PLAN

FLORIDA POWER AND LIGHT COMPANY

TURKEY POINT, UNIT NOS. 3 AND 4

DOCKET NOS. 50-250 AND 50-251

By letter dated July 28, 2010 (Agencywide Documents Access and Management System Accession No. ML102250072), Florida Power and Light Company (the licensee) submitted a license amendment request for the approval of the Turkey Point, Unit Nos. 3 and 4 Cyber Security Plan (CSP). In order to complete the review, the Nuclear Regulatory Commission (NRC) staff needs the following additional information:

**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. Section 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 (DBT).

Enclosure

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 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 that 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**

Section 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 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 Document 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.

March 8, 2011

Mr. Mano Nazar  
Executive Vice President and  
Chief Nuclear Officer  
Florida Power and Light Company  
P.O. Box 14000  
Juno Beach, Florida 33408-0420

SUBJECT: TURKEY POINT UNITS 3 AND 4 - REQUEST FOR ADDITIONAL  
INFORMATION REGARDING AMENDMENT APPLICATION FOR APPROVAL  
OF THE CYBER SECURITY PLAN (TAC NOS. ME4549 AND ME4550)

Dear Mr. Nazar:

By letter dated July 28, 2010, Florida Power & Light Company submitted a license amendment for Turkey Point, Units 3 and 4. The proposed amendment would establish a Cyber Security Plan in conformance with Nuclear Energy Institute (NEI) document NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6, dated April 2010, with three deviations regarding the definition of a Cyber Attack, Emergency Preparedness, and the Turkey Point equivalency of the Senior Nuclear Management as defined in NEI 08-09, Revision 6.

The Nuclear Regulatory Commission (NRC) staff is reviewing the submittal and has determined that additional information is needed to complete its review. The specific questions are found in the enclosed request for additional information (RAI). The NRC staff is requesting a response to the RAI within 30 days of receipt.

If you have any questions regarding this issue, please contact me at (301) 415-5888.

Sincerely,

/RA/

Jason C. Paige, Project Manager  
Plant Licensing Branch II-2  
Division of Operating Reactor Licensing  
Office of Nuclear Reactor Regulation

Docket Nos. 50-250 and 50-251

Enclosure:  
Request for Additional Information

cc w/encl: Distribution via Listserv

DISTRIBUTION:

PUBLIC	RidsNrrLABClayton	RidsAcrsAcnw_MailCTR	LPL2-2R/F
RidsNrrTurkeyPoint	RidsOGCRp	RidsNrrDorlDpr	C. Erlanger, NSIR
RidsRgn2MailCenter	RidsNrrDorlLp12-2	P. Pederson, NSIR	RidsNrrDorlLp13-1
T. Wengert, NRR/DORL	B. Singal, NRR/DORL		

ADAMS Accession No.: ML110630437

\*Memo dated

OFFICE	DORL/LPL2-2/PM	DORL/LPL2-2/LA	NSIR/DSP/BC	DORL/LPL2-2/BC
NAME	JPaige	BClayton	CErlanger*	DBroaddus
DATE	03/08/11	03/07/11	02/18/11	03/08/11

OFFICIAL RECORD COPY