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

March 16, 2011

Mr. Michael R. Glover
General Manager, Nuclear Support
Nuclear Generation
Duke Energy Carolinas, LLC
P.O. Box 1006
Charlotte NC 28201-1106

SUBJECT: CATAWBA NUCLEAR STATION, UNITS 1 AND 2, MCGUIRE NUCLEAR STATION, UNITS 1 AND 2, AND OCONEE NUCLEAR STATION, UNITS 1, 2, AND 3 – REQUEST FOR ADDITIONAL INFORMATION REGARDING CYBER SECURITY PLANS BASED ON NUCLEAR ENERGY INSTITUTE 08-09, REVISION 6 (TAC NOS. ME4529, ME4530, ME4531, ME4532, ME4533, ME4534, AND ME4535)

Dear Mr. Glover:

By letter dated August 16, 2010 (Agencywide Documents Access and Management System, Accession No. ML102300168), you submitted Supplement 2 of your cyber security plans for approval for the Catawba Nuclear Station, Units 1 and 2, the McGuire Nuclear Station, Units 1 and 2, and the Oconee Nuclear Station, Units 1, 2, and 3. Your cyber security plans were based on Nuclear Energy Institute 08-09, Revision 6.

The Nuclear Regulatory Commission staff is reviewing the submittal and has determined that additional information is required to complete its evaluation. This request was discussed with Mr. Jeff Thomas of your staff on March 14, 2011, and it was agreed that a response would be provided within 30 days from the date of this letter.

If you have any questions, please contact me at 301-415-1345.

Sincerely,

John F. Stang, Project Manager
Plant Licensing Branch II-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. 50-413, 50-414, 50-369, 50-370,
50-269, 50-270, and 50-287

Enclosure:
Request for Additional Information

cc w/encl: Distribution via Listserv

REQUEST FOR ADDITIONAL INFORMATION (RAI)

REGARDING CYBER SECURITY PLAN

CATAWBA NUCLEAR STATION, UNITS 1 AND 2

DOCKET NOS. 50-413, AND 50-414

MCGUIRE NUCLEAR STATION, UNITS 1 AND 2

DOCKET NOS. 50-369 AND 50-370

OCONEE NUCLEAR STATION, UNITS 1, 2, AND 3

DOCKET NOS. 50-269, 50-270, AND 50-287

RAI 1: Records Retention

Paragraph (c)(2) of Title 10 of the *Code of Federal Regulations* (10 CFR), Part 73, Section 73.54 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: "the licensee shall retain all records and supporting technical documentation required to satisfy the requirements of this section as a record until the [Nuclear Regulatory] Commission terminates the license for which the records were developed, and shall maintain superseded portions of these records for at least three (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.

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. Paragraph (a) of 10 CFR 73.54 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, except for Watts Bar Nuclear Plant, Unit 2. In order to support the NRC inspection of the implementation prior to issuance of an operating license for Watts Bar Nuclear Plant, Unit 2, the key intermediate milestones shall be completed no later than December 31, 2011. 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

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

March 16, 2011

Mr. Michael R. Glover
General Manager, Nuclear Support
Nuclear Generation
Duke Energy Carolinas, LLC
P.O. Box 1006
Charlotte NC 28201-1106

SUBJECT: CATAWBA NUCLEAR STATION, UNITS 1 AND 2, MCGUIRE NUCLEAR STATION, UNITS 1 AND 2, AND OCONEE NUCLEAR STATION, UNITS 1, 2, AND 3 – REQUEST FOR ADDITIONAL INFORMATION REGARDING CYBER SECURITY PLANS BASED ON NUCLEAR ENERGY INSTITUTE 08-09, REVISION 6 (TAC NOS. ME4529, ME4530, ME4531, ME4532, ME4533, ME4534, AND ME4535)

Dear Mr. Glover:

By letter dated August 16, 2010 (Agencywide Documents Access and Management System, Accession No. ML102300168), you submitted Supplement 2 of your cyber security plans for approval for the Catawba Nuclear Station, Units 1 and 2, the McGuire Nuclear Station, Units 1 and 2, and the Oconee Nuclear Station, Units 1, 2, and 3. Your cyber security plans were based on Nuclear Energy Institute 08-09, Revision 6.

The Nuclear Regulatory Commission staff is reviewing the submittal and has determined that additional information is required to complete its evaluation. This request was discussed with Mr. Jeff Thomas of your staff on March 14, 2011, and it was agreed that a response would be provided within 30 days from the date of this letter.

If you have any questions, please contact me at 301-415-1345.

Sincerely,

/RA/

John F. Stang, Project Manager
Plant Licensing Branch II-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. 50-413, 50-414, 50-369, 50-370,
50-269, 50-270, and 50-287

Enclosure:
Request for Additional Information

cc w/encl: Distribution via Listserv

DISTRIBUTION:

PUBLIC	LPLII-1 R/F	RidsNrrDorlLp2-1 Resource
RidsNrrDirsItsb Resource	RidsNrrDorlDpr Resource	RidsOgcRp Resource
RidsRgn2MailCenter Resource	C. Erlanger, NSIR	T. Wengert, NRR
RidsNrrPMOconee Resource	RidsNrrPMMcGuire Resource	RidsNrrPMCatawba Resource
RidsNrrLAMOBrien Resource	RidsAcrsAcnw_MailCtr Resource	P. Pederson, NSIR

ADAMS Accession No. ML110730243

OFFICE	NRR/LPL2-1/PM	NRR/LPL2-1/PM	NRR/LPL2-1/LA	NRR/LPL2-1/BC	NRR/LPL2-1/PM
NAME	JStang	JThompson	MO'Brien	GKulesa	JStang
DATE	3/11/11	3/16/11	3/16/11	3/16/11	3/16/11

OFFICIAL RECORD COPY