



Serial: NPD-NRC-2009-187
August 13, 2009

10 CFR 73.54

U.S. Nuclear Regulatory Commission
Attention: Document Control Desk
Washington, D.C. 20555-0001

**SHEARON HARRIS NUCLEAR POWER PLANT, UNITS 2 AND 3
NRC DOCKET NOS. 52-022 AND 52-023
CYBER SECURITY PLAN AND PROPOSED IMPLEMENTATION SCHEDULE**

Ladies and Gentlemen:

This letter identifies changes that will be made to a future revision of the Shearon Harris Nuclear Power Plant (HAR) Units 2 and 3 combined license application (COLA) to address Nuclear Regulatory Commission (NRC) requirements in 10 CFR (§) 52.79 (a)(36)(iii – iv) and § 73.54. These requirements are related to providing a cyber security plan and a proposed implementation schedule. The HAR Units 2 and 3 Cyber Security Plan is provided in Attachment A to the enclosure of this letter; a redacted version of the Cyber Security Plan is provided in Attachment B; and a table defining deviations from the generic or standard content of the cyber security plan as developed by the AP1000 Design Centered Working Group (DCWG) is provided in Attachment C; the proposed implementation schedule and other COLA changes related to the Cyber Security Plan are addressed in the enclosure of this letter.

We understand from discussions with members of the NRC's Office of the General Counsel (OGC) and Office of Nuclear Security and Incident Response (NSIR) that cyber security plans do not need to be categorically treated as Safeguards Information (SGI) but instead should be screened to determine whether any information in the plans constitutes SGI in accordance with 10 CFR 73.21. We have reviewed the attached proposed Cyber Security Plan and appendices, and have determined that none of the information in these documents constitutes SGI.

Attachment A to the enclosure of this letter provides the HAR Units 2 and 3 Cyber Security Plan, which contains Security-Related Information, and accordingly is requested to be withheld from public disclosure under 10 CFR 2.390(d).

If you have any further questions, or need additional information, please contact Bob Kitchen at (919) 546-6992, or me at (919) 546-6107.

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

Executed on August 13, 2009.

Sincerely,

Garry D. Miller
General Manager
Nuclear Plant Development

Progress Energy Carolinas, Inc.
P.O. Box 1551
Raleigh, NC 27602

D084
NRO

United States Nuclear Regulatory Commission
NPD-NRC-2009-187
Page 2

Enclosure/Attachments

cc : U.S. NRC Region II, Regional Administrator
U.S. NRC Resident Inspector, SHNPP Unit 1
Mr. Brian Hughes, U.S. NRC Project Manager

**Shearon Harris Nuclear Power Plant Units 2 and 3
Cyber Security Plan and Implementation Schedule**

<u>NRC RAI #</u>	<u>Progress Energy RAI #</u>	<u>Progress Energy Response</u>
None	None	Response enclosed – see following pages

<u>Associated Additional Attachments / Enclosures</u>	<u>Pages Included</u>
Attachment A	Pages 1 – 86
Attachment B	Pages 1 - 3
Attachment C	Pages 1 - 3

**NRC Review of Combined License Application
DISCUSSION OF SHEARON HARRIS NUCLEAR POWER PLANT UNITS 2 AND 3 CYBER
SECURITY PLAN:**

On March 27, 2009, the NRC published the Final Rule related to Power Reactor Security Requirements (RIN 3150-AG63) in the Federal Register (73 FR 13926). 10 CFR 52.79(a)(36)(iii) of the Final Rule requires the final safety analysis report (FSAR) for a combined license (COL) application to include a cyber security plan, in accordance with the criteria set forth in § 73.54. 10 CFR 52.79(a)(36)(iv) requires a description of the implementation of this cyber security plan. This enclosure provides proposed changes to the Shearon Harris Nuclear Power Plant (HAR) Units 2 and 3 combined license application (COLA) related to the cyber security plan, in response to the new requirements discussed above. This information will be included in a future revision to the HAR Units 2 and 3 COLA. Progress Energy Carolinas (PEC) developed the attached site-specific Cyber Security Plan based on the COL Cyber Security Plan template that was developed from the NRC draft template, as described below.

The Nuclear Energy Institute (NEI) has been working with the industry to develop a template (NEI 08-09) for a cyber security plan that would satisfy the requirements of § 73.54 for both the operating reactor fleet and new reactor applicants. To date, the NEI cyber security plan template writing team has been unsuccessful in developing a template that satisfies the NRC Staff's interpretation of the requirements for high assurance that digital computer and communication systems and networks will be adequately protected against cyber attacks, as required by § 73.54. Accordingly, in recognition of the schedule constraints faced by many Combined License (COL) applicants, the Staff developed a draft generic Cyber Security Plan template that provides an acceptable method for compliance with the high assurance requirements set forth in § 73.54. The Staff issued this draft template to the COL applicants on July 8, 2009, encouraging COL applicants to use this template as the basis for their Cyber Security Plans.

Utilizing the NRC's draft Cyber Security Plan template as its foundation, the AP1000 Design-Centered Working Group (DCWG) developed a generic COL Cyber Security Plan template that achieves high assurance of adequate protection from cyber attacks for new reactor facility designs. This COL Cyber Security Plan uses a phased approach to developing and validating the technology-standard and site-specific "baseline" technical, operational, and management cyber security controls, defensive strategies, and attack mitigation methods. Each project phase uses available information on cyber security controls and programmatic implementation to further refine, develop, and document the Cyber Security Program with the goal of integrating cyber security controls and strategies across the established security, design control, configuration management, and assessment/oversight programs. The COL Cyber Security Plan implements a Cyber Security Program to maintain the established cyber security controls through a comprehensive life cycle approach. Similar to the NRC's draft plan, the COL plan also addresses the ongoing management and assessment, change control, security program review, document control, records retention, and document/records handling, and reporting requirements of an effective cyber security program.

Pursuant to the new requirements in 10 CFR 52.79(a)(36)(iii), Attachment A to this enclosure provides the HAR Units 2 and 3 Cyber Security Plan. **The site-specific Cyber Security Plan in Attachment A contains Security-Related Information, and accordingly should be withheld from public disclosure under 10 CFR 2.390(d).** Attachment B contains a redacted version of the HAR Units 2 and 3 Cyber Security Plan, which consists of the cover sheet only.

Attachment C contains a table defining site-specific deviations from the standard content of the cyber security plan as developed by the AP1000 Design Centered Working Group (DCWG).

PEC will incorporate the full, non-redacted version of the Cyber Security Plan, including any applicable changes identified in response to NRC requests for additional information or other change drivers, in a future revision of COLA Part 9, Withheld Information. The redacted version of this Cyber Security Plan will be incorporated into a future revision to COLA Part 11, Enclosures. The Cyber Security Plan describes the operational Cyber Security Program required by § 73.54.

The proposed implementation schedule for the HAR Units 2 and 3 Cyber Security Program, as addressed in the changes to COLA Parts 2 and 10 below (FSAR Table 13.4 – 201 and proposed License Condition 3.G.10, respectively), provides for a fully implemented program prior to initial fuel load.

The COLA changes related to the submittal of the Cyber Security Plan also include FSAR changes to provide a reference to §52.79(a)(36) as a basis for incorporating the Cyber Security Plan as a licensing document and to delete the reference to NEI 04-04, Revision 1. With the incorporation of the changes in PEC's May 4, 2009, letter (NPD-NRC-2009-086, Reference 1), and the deletion of this reference (Reference 202), there are no remaining references in Section 13.6.2. Accordingly, Subsection 13.6.2 is deleted in its entirety.

Southern Nuclear Operating Company's (SNC) Vogtle Electric Generating Station (VEGP) Units 3 and 4 is the R-COLA for issues associated with the Final Rule related to Power Reactor Security Requirements. The VEGP Units 3 and 4 proposed Cyber Security Plan, which was developed based upon the COL Cyber Security Plan template, was submitted for NRC review on July 24, 2009 (Reference 2). The attached HAR Units 2 and 3 Cyber Security Plan was written to conform to the generic and standard content in the VEGP Units 3 and 4 proposed Cyber Security Plan. Consequently, the generic and standard text in the HAR Cyber Security Plan is the same as that in the R-COLA Cyber Security Plan, with the exception of deviations identified in Attachment C. Site-specific information is identified as blue, bracketed text in the VEGP Cyber Security Plan Reviewer's Aid that was provided to the NRC by letter dated August 3, 2009 (Reference 3). This site-specific information in the HAR Units 2 and 3 Cyber Security Plan may differ from that in the VEGP Units 3 and 4 Cyber Security Plan.

The change to COLA Part 2, FSAR, resulting from COL Application Revision 1 below is in agreement with the VEGP Units 3 and 4 FSAR revision provided in SNC's letter dated July 24, 2009 (Reference 2). The changes provided by COL Application Revisions 2 and 3 below are consistent with the current text in the corresponding sections of the VEGP FSAR. Therefore, these FSAR changes are expected to be STANDARD information.

ASSOCIATED HAR COL APPLICATION REVISIONS:

1. Change COLA Part 2, FSAR, Section 13.6, Security, third and fourth paragraphs:

Current text:

An operational program following the guidance of NRC endorsed NEI 04-04 Revision 1 (Reference 202) will be implemented prior to fuel load.

Table 13.4-201 provides milestones for security program implementation.

To read:

The Cyber Security Plan is submitted to the Nuclear Regulatory Commission as a separate licensing document to fulfill the requirements contained in 10 CFR 52.79(a)(36) and 10 CFR 73.54. The Cyber Security Plan will be maintained in accordance with the requirements of 10 CFR 52.98. The Plan is withheld from public disclosure pursuant to 10 CFR 2.390.

Table 13.4-201 provides milestones for security program and cyber security program implementation.

2. Delete COLA Part 2, FSAR, Subsection 13.6.2, REFERENCES, in its entirety. A change in PEC's letter dated May 4, 2009 (Reference 1), deleted Reference 201, NEI 03-12, Appendix F. The change addressed by this letter supplements the change to delete Reference 201 by also deleting Reference 202, NEI 04-04, and consequently deletes the entire subsection.
3. Change COLA Part 2, FSAR, Table 13.4-201, by separating the Fitness for Duty (FFD) Program (Line item 20) from the Security Program (Line item 15), and adding a new Line item 21 for the Cyber Security Program. Table 13.4-201 is also changed to clarify that the Security Program implementation milestone is "Prior to receipt of fuel onsite (protected area)," and the Fitness for Duty Program construction milestone is "Prior to initiating onsite construction," in conformance with the Final Rule related to Power Reactor Security Requirements.

Current text:

Item	Program Title	Program Source (Required by)	FSAR Section	Implementation	
				Milestone	Requirement
15.	Security Program:	10 CFR 50.34(c);			
	Physical Security Program	10 CFR 73.55; 10 CFR 73.56; 10 CFR 73.57;	13.6	Prior to receipt of fuel onsite	License Condition
	Safeguards Contingency Program	10 CFR 50.34(d)	13.6	Prior to receipt of fuel onsite	License Condition
	Training and Qualification Program	10 CFR Part 73, Appendix C	13.6	Prior to receipt of fuel onsite	License Condition
	Fitness for Duty Program (Construction – Mgt. & Oversight Personnel)	10 CFR Part 26 Subparts A-H, N, and O	13.7	Prior to initiating construction	License Condition
	Fitness for Duty Program (Construction – Workers & First Line Supv.)	10 CFR Part 26 Subparts K	13.7	Prior to initiating construction	License Condition

Fitness for Duty Program (Operation)	10 CFR Part 26	13.7	Prior to initial fuel load	License Condition
---	----------------	------	-------------------------------	----------------------

To read:

Item	Program Title	Program Source (Required by)	FSAR Section	Implementation	
				Milestone	Requirement
15.	Security Program:	10 CFR 50.34(c);			
	Physical Security Program	10 CFR 73.55; 10 CFR 73.56; 10 CFR 73.57;	13.6	Prior to receipt of fuel onsite (protected area)	License Condition
	Safeguards Contingency Program	10 CFR 50.34(d) 10 CFR Part 73, Appendix C	13.6	Prior to receipt of fuel onsite (protected area)	License Condition
	Training and Qualification Program	10 CFR Part 73, Appendix B	13.6	Prior to receipt of fuel onsite (protected area)	License Condition
20.	Fitness For Duty Programs:				
	Fitness for Duty Program (Construction – Mgt. & Oversight Personnel)	10 CFR Part 26 Subparts A-H, N, and O	13.7	Prior to initiating onsite construction	License Condition
	Fitness for Duty Program (Construction – Workers & First Line Supv.)	10 CFR Part 26 Subparts K	13.7	Prior to initiating onsite construction	License Condition
	Fitness for Duty Program (Operation)	10 CFR Part 26	13.7	Prior to initial fuel load	License Condition
21.	Cyber Security Program	10 CFR 73.54	13.6	Prior to initial fuel load	License Condition

4. Change COLA Part 9, Withheld Information, to include the Cyber Security Plan (as provided in Attachment A), which contains security-related information, and therefore, should be withheld in accordance with 10 CFR 2.390(d). PEC will incorporate the full, non-redacted version of the Cyber Security Plan, including any applicable changes identified in response to NRC requests for additional information or other change drivers, in a future revision of COLA Part 9, Withheld Information.

5. Change COLA Part 10, Proposed License Conditions (Including ITAAC), by adding the Cyber Security Program to the list of operational programs that are required to be

implemented prior to initial fuel load. The following will be inserted after the programs currently listed under Proposed License Condition 3.G, Fuel Loading:

G.10 – Cyber Security

6. Change COLA Part 11, Enclosures, by including the new Cyber Security Plan (as provided in Attachment B). Note: The actual Plan is requested to be withheld from disclosure in accordance with 10 CFR 2.390(d), because it contains security-related information. Consequently, the version of the HAR Units 2 and 3 Cyber Security Plan in Part 11 is redacted, and the full document is provided in COLA Part 9, Withheld Information.

ASSOCIATED ATTACHMENTS/ENCLOSURES:

- Attachment A Shearon Harris Nuclear Power Plant, Units 2 and 3; Cyber Security Plan (Non-Public Version) (86 pages, including cover page)
- Attachment B Shearon Harris Nuclear Power Plant, Units 2 and 3; Cyber Security Plan (Public Version - Redacted) (3 pages, including cover page)
- Attachment C Table of Deviations from AP1000 R-COLA Cyber Security Plan (3 pages, including cover page)

NOTE: Attachment A contains Security-Related Information - Withhold Under 10 CFR 2.390(d).

REFERENCES:

1. Letter from Garry D. Miller (PEC) to NRC Document Control Desk "Shearon Harris Nuclear Power Plant, Units 1 and 2, Dockets Nos. 52-022 and 52-023, Changes to Fitness for Duty Program Information, Physical Security During Construction, and Physical Security Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC)," NPD-NRC-2009-086, dated May 4, 2009
2. Letter from Charles R. Pierce (SNC) to NRC Document Control Desk, "Southern Nuclear Operating Company, Vogtle Electric Generating Plant Units 3 and 4 Combined License Application, Proposed Cyber Security Plan and Proposed Implementation Schedule," dated July 24, 2009.
3. Letter from Charles R. Pierce (SNC) to NRC Document Control Desk, "Southern Nuclear Operating Company, Vogtle Electric Generating Plant Units 3 and 4 Combined License Application, Proposed Cyber Security Plan – Reviewer's Aid," dated August 3, 2009.

ATTACHMENT B

SHEARON HARRIS NUCLEAR POWER PLANT
UNITS 2 AND 3

CYBER SECURITY PLAN

(PUBLIC VERSION - REDACTED)

(3 pages, including this cover)

PROGRESS ENERGY CAROLINAS, INC.

**Shearon Harris Nuclear Power
Plant, Units 2 & 3**

Cyber Security Plan

August 2009

**Security-Related Information - Withheld Under 10 CFR 2.390(d)
(See Part 9 of this COL Application)**

ATTACHMENT C

SHEARON HARRIS NUCLEAR POWER PLANT
UNITS 2 AND 3

TABLE OF DEVIATIONS FROM AP 1000 R-COLA
CYBER SECURITY PLAN

(PUBLIC VERSION - REDACTED)

(3 pages, including this cover)

Shearon Harris Nuclear Power Plant Units 2 and 3

Table of Deviations from Standard and Generic text of AP1000 R-COLA Cyber Security Plan

(submitted by Southern Nuclear Operating Company for Vogtle Electric Generating Plant, Units 3 and 4, on July 24, 2009)

Plan Section (Cyber Security Plan or Appendix and Number)	Deviation Type (Generic or AP1000 Standard)	Previous Text	New Text	Justification Summary
Cyber Security Plan Section 2.1, second paragraph first numbered bullet (page 1)	Generic	Section 3.1.6	Section 3	The reference was incorrect. The new text points to the intended section.
Cyber Plan section 3.1.2, first paragraph eighth bullet, (page 5)	Standard	"a emergency"	"an emergency"	Corrected for grammar and clarity
Cyber Security Plan Section 3.1.2, first paragraph eleventh bullet (page 5)	Standard	APP-GW-E1-006, AP1000 "Cyber Security Design Criteria"	APP-GW-E1-006, "AP1000 Cyber Security Design Criteria"	Typo
Cyber Security Plan Section 3.1.3, first paragraph (page 6)	Standard	APP-GW-J0H-001, AP1000 I&C Cyber Security Plan.	APP-GW-J0H-001, "AP1000 I&C Cyber Security Plan."	Punctuation correction
Cyber Plan. Table of Contents. (Page ii)	Standard	Section 6 second level items missing	Added 6.1 and 6.2 to the TOC	Consistency with TOC hierarchy.
Appendix C Section 5.5, second bullet (page C-10)	Standard	enforceing	enforcing	Spelling correction
Appendix C Section 7, sixth bullet (page C-12)	Standard	eliminated/restricted with justification that explains that communication from a lower security level to a higher security level verifies that a compromise of such	eliminated/restricted with adequate justification explaining how a compromise of such communication from a lower security level to a higher security level will not prevent or degrade	Corrected grammar and readability

Plan Section (Cyber Security Plan or Appendix and Number)	Deviation Type (Generic or AP1000 Standard)	Previous Text	New Text	Justification Summary
		communication will not prevent or degrade the functions performed by the CDAs in the higher security level.	the functions performed by the CDAs in the higher security level.	
Appendix C Section 11.5, first paragraph (page C-27)	Standard	Section 3	Section 4	The reference was incorrect. The new text points to the intended section.