



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

February 25, 2011

Mr. Thomas D. Gatlin
Vice President, Nuclear Operations
South Carolina Electric & Gas Company
Virgil C. Summer Nuclear Station
Post Office Box 88
Jenkinsville, SC 29065

**SUBJECT: VIRGIL C. SUMMER NUCLEAR STATION, UNIT NO. 1 (SUMMER) –
REQUEST FOR ADDITIONAL INFORMATION (RAI) ON CYBER SECURITY
PROGRAM (TAC NO. ME4553)**

Dear Mr. Gatlin:

By letter dated August 5, 2010 (Agencywide Documents Access and Management System (ADAMS), Accession No. ML102210192), South Carolina Electric and Gas Company (SCE&G) submitted of a license amendment request for U.S. Nuclear Regulatory Commission (NRC) review and approval of a facility cyber security program (CSP) and proposed implementation schedule for Summer. The NRC staff has determined that additional information is required to address the issues of records retention, implementation schedules and the scoping of systems in the CSP, as discussed in further detail in the Enclosure. The NRC staff has determined that no security-related or proprietary information is contained therein.

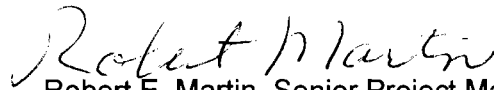
We understand that the Nuclear Energy Institute and the industry Cyber Security Task Force are working to ensure that operating reactor licensees will submit consistent responses to the NRC for these generic RAIs. The NRC staff believes that consistency in the implementation of NRC regulations across the licensed power reactor fleet supports the protection of the public health and safety.

T. Gatlin

-2-

We request that a response be provided within 30 days of the date of this letter.

Sincerely,

A handwritten signature in black ink that reads "Robert E. Martin". The signature is written in a cursive style with a large, prominent "R" at the beginning.

Robert E. Martin, Senior Project Manager
Plant Licensing Branch II-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-395

Enclosure:
RAI

cc w/encl: Distribution via Listserv

REQUEST FOR ADDITIONAL INFORMATION
REGARDING THE LICENSE AMENDMENT REQUEST
TO IMPLEMENT A CYBER SECURITY PROGRAM AT
VIRGIL C. SUMMER NUCLEAR STATION, UNIT NO. 1
TAC NO. ME4553

RAI 1: Records Retention

Title 10 of the *Code of Federal Regulations* (10 CFR) Paragraph 73.54(c)(2) requires licensees to design a cyber security program (CSP) 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 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. Paragraph 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.

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. The key CSP implementation milestones are as follows:

Enclosure

- (a) Establish, train and qualify a 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, for example, 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 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 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.

T. Gatlin

- 2 -

We request that a response be provided within 30 days of the date of this letter.

Sincerely,

/RA/

Robert E. Martin, Senior Project Manager
Plant Licensing Branch II-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-395

Enclosure:
RAI

cc w/encl: Distribution via Listserv

DISTRIBUTION

PUBLIC	LPL2-1 R/F	RidsAcrsAcnw_MailCTR Resource
RidsNrrDorIDpr Resource	RidsNrrDorLpl2-1 Resource	RidsRgn2MailCenter Resource
RidsNrrLAMOBrienResource	RidsOgcRp Resource	RidsNsirDsp Resource
PPederson, NSIR	CErlanger, NSIR	RidsNrrPMSummer Resource

ADAMS Accession Number: ML110540479

*by memo dated 2/18/11

OFFICE	LPL2-1/PM	LPL2-1/LA	NSIR/DSP/BC	LPL2-1/BC	LPL2-1/PM
NAME	RMartin	MO'Brien	CErlanger *	GKulesa (JStang for)	RMartin
DATE	02 /24/11	02/24/11	2/18/11	02/25/11	02/25/11

OFFICIAL RECORD COPY