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

March 9, 2017

Mr. George A. Lippard, III
Vice President, Nuclear Operations
South Carolina Electric & Gas Company
Virgil C. Summer Nuclear Station
P.O. Box 88, Mail Code 800
Jenkinsville, SC 29065

SUBJECT: VIRGIL C. SUMMER NUCLEAR STATION, UNIT NO. 1 – ISSUANCE OF AMENDMENT TO REVISE COMPLETION DATE OF IMPLEMENTATION MILESTONE 8 OF THE CYBER SECURITY PLAN (CAC NO. MF8074)

Dear Mr. Lippard:

The U.S. Nuclear Regulatory Commission (the Commission) has issued the enclosed Amendment No. 208 to Renewed Facility Operating License (RFOL) No. NPF-12 for the Virgil C. Summer Nuclear Station, Unit No. 1 (VCSNS), in response to your application dated June 30, 2016, as supplemented by letter dated August 4, 2016. This amendment revises license conditions Paragraph 2.C.(2) and Paragraph 2.E of the RFOL. Specifically, the amendment revises the Milestone 8 completion date of the Cyber Security Plan implementation schedule. Milestone 8 requires full implementation of the VCSNS Cyber Security Plan.

A copy of the related Safety Evaluation is also enclosed. Notice of Issuance will be included in the Commission's biweekly *Federal Register* notice.

Sincerely,

Shawn Williams

Shawn A. Williams, Senior Project Manager
Plant Licensing Branch II-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-395

Enclosures:
1. Amendment No. 208 to NPF-12
2. Safety Evaluation

cc w/Enclosures: Distribution via Listserv

SUBJECT: VIRGIL C. SUMMER NUCLEAR STATION, UNIT NO. 1 – ISSUANCE OF AMENDMENT TO REVISE COMPLETION DATE OF IMPLEMENTATION MILESTONE 8 OF THE CYBER SECURITY PLAN (CAC NO. MF8074) DATED MARCH 9, 2017

DISTRIBUTION:

PUBLIC LPL2-1 R/F	RidsNrrPMSummer Resource
RidsACRS_MailCTR Resource	RidsDssSbpb Resource
RidsNrrDorlLpl2-1 Resource	RidsRgn2MailCenter Resource
RidsNrrLAKGoldstein Resource	RecordsAmend
RidsNrrDssStsb Resource	JRycyna, NSIR

ADAMS Accession No.: ML17011A050 *by internal email

OFFICE	DORL/LPL2-1/PM	DORL/LPL2-1/LA	NSIR/CSD/ABC*	OGC/HLW
NAME	SWilliams	KGoldstein	JBeardsley	PJehle NLO w/edits
DATE	01/27/17	03/13/17	01/05/17	02/24/17
OFFICE	DORL/LPL2-1/BC	DORL/LPL2-1/PM		
NAME	MMarkley	SWilliams		
DATE	03/09/17	03/09/17		

OFFICIAL RECORD COPY

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

SOUTH CAROLINA ELECTRIC & GAS COMPANY

SOUTH CAROLINA PUBLIC SERVICE AUTHORITY

DOCKET NO. 50-395

VIRGIL C. SUMMER NUCLEAR STATION, UNIT NO. 1

AMENDMENT TO RENEWED FACILITY OPERATING LICENSE

Amendment No. 208
Renewed License No. NPF-12

1. The U.S. Nuclear Regulatory Commission (the Commission) has found that:

   A. The application for amendment to the Virgil C. Summer Nuclear Station, Unit No. 1 (the facility), Renewed Facility Operating License No. NPF-12 filed by the South Carolina Electric & Gas Company (the licensee), dated June 30, 2016, as supplemented by letter dated August 4, 2016, complies with the standards and requirements of the Atomic Energy Act of 1954, as amended (the Act), and the Commission's rules and regulations set forth in 10 CFR Chapter I;

   B. The facility will operate in conformity with the application, the provisions of the Act, and the rules and regulations of the Commission;

   C. There is reasonable assurance (i) that the activities authorized by this amendment can be conducted without endangering the health and safety of the public, and (ii) that such activities will be conducted in compliance with the Commission's regulations as set forth in 10 CFR Chapter I;

   D. The issuance of this amendment will not be inimical to the common defense and security or to the health and safety of the public; and

   E. The issuance of this amendment is in accordance with 10 CFR Part 51 of the Commission's regulations and all applicable requirements have been satisfied.

2. Accordingly, the license is amended as indicated in the attachment to this license amendment. Paragraph 2.C.(2) and Paragraph 2.E of Renewed Facility Operating License No. NPF-12 is hereby amended to read as follows:

2.C.(2) Technical Specifications and Environmental Protection Plan

The Technical Specifications contained in Appendix A, as revised through Amendment No. 208, and the Environmental Protection Plan contained in Appendix B, are hereby incorporated in the license. South Carolina Electric & Gas Company shall operate the facility in accordance with the Technical Specifications and the Environmental Protection Plan.

2.E SCE&G shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The SCE&G CSP was approved by License Amendment No. 184, as supplemented by changes approved by License Amendment Nos. 198 and 208.

3. This amendment is effective as of its date of issuance and shall be implemented within 60 days of issuance.

FOR THE NUCLEAR REGULATORY COMMISSION

Michael T. Markley, Chief
Plant Licensing Branch II-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Attachment:
Changes to Renewed Facility
Operating License

Date of Issuance: March 9, 2017

VIRGIL C. SUMMER NUCLEAR STATION, UNIT NO. 1

ATTACHMENT TO LICENSE AMENDMENT NO. 208

RENEWED FACILITY OPERATING LICENSE NO. NPF-12

DOCKET NO. 50-395

Replace the following page of the Renewed Facility Operating License with the attached revised pages. The revised pages are identified by amendment number and contain marginal lines indicating the areas of change.

Remove	Insert
License	License
Page 3	Page 3
Page 11a	Page 11a

(3) SCE&G, pursuant to the Act and 10 CFR Part 70, to receive, possess and use at any time special nuclear material as reactor fuel, in accordance with the limitations for storage and amounts required for reactor operation, as described in the Final Safety Analysis Report, as amended through Amendment No. 33;

(4) SCE&G, pursuant to the Act and 10 CFR Parts 30, 40 and 70, to receive, possess and use at any time any byproduct, source and special nuclear material as sealed neutron sources for reactor startup, sealed neutron sources for reactor instrumentation and radiation monitoring equipment calibration, and as fission detectors in amounts as required;

(5) SCE&G, pursuant to the Act and 10 CFR Parts 30, 40 and 70, to receive, possess and use in amounts as required any byproduct, source or special nuclear material without restriction to chemical or physical form, for sample analysis or instrument calibration or associated with radioactive apparatus or components; and

(6) SCE&G, pursuant to the Act and 10 CFR Parts 30, 40 and 70, to possess, but not separate, such byproduct and special nuclear materials as may be produced by the operation of the facility.

C. This renewed license shall be deemed to contain, and is subject to, the conditions specified in the Commission's regulations set forth in 10 CFR Chapter I and is subject to all applicable provisions of the Act and to the rules, regulations, and orders of the Commission now or hereafter in effect; and is subject to the additional conditions specified or incorporated below:

(1) Maximum Power Level

SCE&G is authorized to operate the facility at reactor core power levels not in excess of 2900 megawatts thermal in accordance with the conditions specified herein and in Attachment 1 to this renewed license. The preoperational tests, startup tests and other items identified in Attachment 1 to this renewed license shall be completed as specified. Attachment 1 is hereby incorporated into this license.

(2) Technical Specifications and Environmental Protection Plan

The Technical Specifications contained in Appendix A, as revised through Amendment No. 208, and the Environmental Protection Plan contained in Appendix B, are hereby incorporated in the license. South Carolina Electric & Gas Company shall operate the facility in accordance with the Technical Specifications and the Environmental Protection Plan.

D. An exemption to the requirements of Paragraph III.B.4 of Appendix G to 10 CFR Part 50 is described in Section 5.3.1 of Supplement No. 1 to the Office of Nuclear Reactor Regulation's Safety Evaluation Report. A limited exemption to the requirements of Section IV.F.1(b) of Appendix E to 10 CFR Part 50 is described in a letter from B. J. Youngblood, NRC to O. W. Dixon, Jr., dated November 2, 1982. These exemptions are authorized by law and will not endanger life or property or the common defense and security and are otherwise in the public interest. The facility will operate, to the extent authorized herein, in conformity with the application, as amended, the provisions of the Act, and the rules and regulations of the Commission.

E. SCE&G shall fully implement and maintain in effect all provisions of the Commission-approved physical security, training and qualification, and safeguards contingency plans including amendments made pursuant to provisions of the Miscellaneous Amendments and Search Requirements revisions to 10 CFR 73.55 (51 FR 27817 and 27822) and to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The combined set of plans, which contain Safeguards Information protected under 10 CFR 73.21, is entitled: "Virgil C. Summer Nuclear Station Security Plan," as updated through May 15, 2006. This document includes the Security Training and Qualification Plan as Appendix B and the Safeguards Contingency Plan as Appendix C.

SCE&G shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The SCE&G CSP was approved by License Amendment No. 184, as supplemented by changes approved by License Amendment Nos. 198 and 208.

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

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO AMENDMENT NO. 208 TO

RENEWED FACILITY OPERATING LICENSE NO. NPF-12

SOUTH CAROLINA ELECTRIC & GAS COMPANY

SOUTH CAROLINA PUBLIC SERVICE AUTHORITY

VIRGIL C. SUMMER NUCLEAR STATION, UNIT NO. 1

DOCKET NO. 50-395

1.0 INTRODUCTION

By letters dated June 30, 2016 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML16188A105), supplemented by letter dated August 4, 2016 (ADAMS Accession No. ML16221A034), South Carolina Electric & Gas Company (SCE&G, the licensee) requested a change to the facility operating license (FOL) for the Virgil C. Summer Nuclear Station, Unit 1 (VCSNS).

This amendment revises license conditions Paragraph 2.C.(2) and Paragraph 2.E of the Renewed Facility Operating License. Specifically, the amendment revises the Milestone 8 completion date of the Cyber Security Plan implementation schedule. Milestone 8 requires full implementation of the VCSNS Cyber Security Plan.

The letters dated June 30, 2016, and August 4, 2016, contained enclosures that were submitted as sensitive security-related information under Title 10 of the *Code of Federal Regulations* (10 CFR) 2.390, and, accordingly those portions are withheld from public disclosure.

The supplement dated August 4, 2016, provided additional information that clarified the application, did not expand the scope of the application as originally noticed, and did not change the Nuclear Regulatory Commission (NRC or the Commission) staff's original proposed no significant hazards consideration determination as published in the *Federal Register* on October 4, 2016 (81 FR 68472).

2.0 REGULATORY EVALUATION

Regulatory Requirements and Guidance

The NRC staff considered the following regulatory requirements and guidance in its review of the current license amendment request to extend the existing CSP implementation schedule:

- 10 CFR 73.54 states: "Each [CSP] submittal must include a proposed implementation schedule. Implementation of the licensee's cyber security program must be consistent with the approved schedule

- Amendment No. 184 dated August 24, 2011 (ADAMS Accession No. ML11201A312),which approved the licensee's CSP and implementation schedule, included the following statement: "The licensee shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p)."

- In a publically available NRC memorandum dated October 24, 2013 (ADAMS Accession No. ML13295A467), the NRC staff listed criteria that it would consider during its evaluations of licensees' requests to postpone their cyber security program implementation date (Milestone 8).

The NRC staff does not regard the CSP milestone implementation dates as regulatory commitments that can be changed unilaterally by the licensee, particularly in light of the regulatory requirement at 10 CFR 73.54, that "[i]mplementation of the licensee's cyber security program must be consistent with the approved schedule." As the NRC staff explained in its letter to all operating reactor licensees dated May 9, 2011 (ADAMS Accession No. ML110980538), the implementation of the plan, including the key intermediate milestone dates and the full implementation date shall be in accordance with the implementation schedule submitted by the licensee and approved by the NRC. All subsequent changes to the NRC-approved CSP implementation schedule, thus, will require prior NRC approval as required by 10 CFR 50.90 "Application for amendment of license, construction permit, or early site permit."

3.0 TECHNICAL EVALUATION

3.1 Licensee's Requested Change

The NRC staff issued Amendment No. 184 to Facility Operating License NPF-12 for VCSNS Unit 1 (ADAMS Accession No. ML11201A312) dated August 24, 2011. This amendment approved the CSP and associated implementation schedule, and added a license condition requiring the licensee to fully implement and maintain the Commission-approved CSP. The implementation schedule was based on a template prepared by the Nuclear Energy Institute (NEI), which was transmitted to the NRC by letter dated February 28, 2011 (ADAMS Accession No. ML110600206). By letter dated March 1, 2011, the NRC staff found the NEI template acceptable for licensees to use to develop their CSP implementation schedules (ADAMS Accession No. ML110070348). Subsequently, NRC staff approved Amendment No. 198, dated May 29, 2014 (ADAMS Accession No. ML14122A309), which extended the VCSNS Milestone 8 implementation to June 30, 2017. In the June 30, 2016 application, SCE&G requested to further extend the Milestone 8 implementation to December 31, 2017.

The licensee's proposed implementation schedule for the Cyber Security Program identified completion dates and bases for the following eight milestones:

1. Establish the Cyber Security Assessment Team (CSAT);
2. Identify Critical Systems (CSs) and Critical Digital Assets (CDAs);
3. Install deterministic one-way devices between lower level devices and higher level devices;
4. Implement the security control "Access Control For Portable And Mobile Devices";
5. Implement observation and identification of obvious cyber related tampering to existing insider mitigation rounds by incorporating the appropriate elements;
6. Identify, document, and implement technical cyber security controls in accordance with Mitigation of Vulnerabilities and Application of Cyber Security Controls for CDAs that could adversely impact the design function of physical security target set equipment;
7. Ongoing monitoring and assessment activities for those target set CDAs whose security controls have been implemented; and
8. Fully implement the CSP.

Currently, Milestone 8 of the licensee's CSP requires VCSNS to fully implement the CSP by June 30, 2017, per Amendment No. 198. In the licensee's June 30, 2016, application, SCE&G proposed to change the Milestone 8 completion date to December 31, 2017. The licensee's supplement dated August 4, 2016, addressed the 8 criteria in the NRC's October 24, 2014 guidance memorandum.

The licensee provided information pertinent to each of the criteria identified in the NRC guidance memorandum. NRC staff notes that information contained in Section 3.1 below was included in the non-public security related enclosure of the August 4, 2016 supplement, The NRC staff determined information presented here is publically available.

Criteria 1 Identification of the specific requirement or requirements of the cyber security plan that the licensee needs additional time to implement.

In response to Criteria 1, the licensee stated that they need additional time to implement CSP Section 3.1.6, *Analyzing Digital Computer Systems and Networks and Applying Cyber Security Controls* and seven subsections of CSP Section 4.0, *Establishing, Implementing, and Maintaining the Cyber Security Program,* specifically to clarify interpretation of security controls and methods.

Criteria 2 Detailed justification that describes the reason the licensee requires additional time to implement the specific requirement or requirements identified.

In response to Criteria 2, the licensee provided the following justification for its request for additional time to implement CSP Section 3.1.6, *Analyzing Digital Computer Systems and Networks and Applying Cyber Security Controls:*

1) Resolution of Industry/NEI/NRC discussion on CDA scope/security controls:

   - CDA/security controls scope changes will impact M8 completion:

   - Scope changes concerning CDA identification and security controls will require significant rework such as: changes to newly issued

procedures and updating existing procedures; revision of training materials and delivery of training; CDA Assessment Tool rework, programming and validation; rework to adjust completed CDA tabletop work; rework of the completed Security Controls Implementation Strategy (SCIS), which is on-hold pending the outcome of NEI/NRC discussions concerning NEI 13-10, *Cyber Security Control Assessments.*

2) Defining the cyber security controls in NEI 08-09:

- Differing industry interpretation of CDA scope and security controls (i.e., no defined criteria of "What good looks like" for security controls).

3) CDA Assessment rework, which includes NEI 13-10 assessments, is resource intensive:

- VCSNS Unit 1 has approximately 1700 CDAs
- Assessment Tool set-up is challenging due to uncertainty surrounding security controls interpretation. The assessment tool vendor has to develop software versions based on the continuing changes to CDA consequence and types based on NEI 13-10, which is now on revision 4 with revision 5 currently being developed.
- VCSNS Unit 1 underestimated the level of effort necessary to address security controls using the deterministic criteria in CSP 3.1.6
- VCSNS Unit 1 has increased permanent staff resources to cope with the magnitude of work involved in program implementation and full program support. New hires have to be trained and mentored.

4) Remediation activities need to be carefully considered.

- Security controls modifications are unique and new to the plant and suppliers.
- Plant modifications must be carefully implemented to ensure they do not impact plant safety and operation.

5) Change management challenges:

Cyber security creates additional challenges due to its integration into daily plant operations, maintenance, engineering and procurement activities. Integration of cyber security controls is taking longer than expected due to impacts on the work control process and maintenance activities. Cyber security for plant CDAs is new, and the security controls being implemented on the plant CDAs are new to

Maintenance, System Engineering and Operations. When plant CDA modifications include new products such as application whitelisting, and require operating system parameter changes, the modifications must be implemented cautiously to ensure safe reliable operation of plant equipment. Before modifications are implemented, significant verification analysis and testing must be performed to minimize or eliminate impacts to plant equipment. Maintenance on CDAs is performed by trained and qualified technicians. Maintenance Department training schedules are normally established at least a year in advance. Additional time to implement Milestone 8 allows more opportunity to complete training without disrupting schedules. Plant modifications that added cyber security controls have created new change management challenges. As cyber security controls are implemented, new tasks are added to normal maintenance activities. The full impact of cyber security controls on the maintenance processes are difficult to predict when plant modifications to add cyber controls are initially scoped and developed.

Extending the implementation date to December 31, 2017, will provide SCE&G additional time to address the resolutions developed for NEI 13-10 workshop based questions. The resolution of these issues is expected to be addressed and resolved through the Security Frequently Asked Question (SFAQ) process or through revisions to current industry guidance documents.

The licensee provided the following justification for its request for additional time to implement CSP Section 4.0, *Establishing, Implementing, and Maintaining the Cyber Security Program:*

1) Section 4.2, *Cyber Security Controls*: Many security controls have actions that are required to be performed on specific frequencies. The frequency of a security control is met if the action is performed within 1.25 times the frequency specified in the control, as applied, and as measured from the previous performance of the action. VCS Unit 1 is currently in the process of identifying and developing the preventive maintenance task requirements. This includes who will perform the task, how the task is performed and how the task is created. How the task is performed can be either automated or manual. Many tasks will rely on the implementation of the Cyber Security Monitoring System discussed below in Section 8. How the task is created is a process that needs to be well planned as to not create rework or extra work that is not required. Is the task written against a single CDA or a Critical System? Once the details are defined many will need to have CSAT approval to proceed.

2) Section 4.3, *Defense-In-Depth Protective Strategies*: VCS is currently developing and issuing an engineering change package to implement a Cyber Security Monitoring System to comply with Section 4.3 of their Cyber Security Plan. The outage related work will occur during the spring of 2017. The implementation time frame leaves VCSNS Unit 1 with very little margin for error with our current MS8 date of June 30, 2017.

3) Section 4.4, *Ongoing Monitoring and Assessment*: Industry, NEI and the NRC are currently holding workshops on Section 4.4 of NEI 08-09 Rev 6. The outcome of these meetings will impact program processes and procedures required to meet the NRC's expectations.

4) Section 4.6, *Attack Mitigation and Incident Response*: VCSNS Unit 1 has developed a draft procedure for Incident Response that aligns with NEI 08-09 Rev 6 requirements and integrates with the changes recently made for 10 CFR 73.77. To implement a compliant program resources from other areas of SCANA Corporation must be utilized. VCSNS Unit 1 is currently developing Interface agreements to support this program.

5) Section 4.7, *Cyber Security Contingency Plan:* VCSNS Unit 1 has developed a draft procedure to implement NEI 08-09 Appendix "E" E-8. Similar to Section 4.6 VCSNS Unit 1 must include other SCANA resources to implement a compliant program.

6) Section 4.10, *Policies and Implementing Procedures:* As stated previously VCSNS Unit 1 has created multiple draft procedures that are awaiting the outcome of SFAQs, Industry/NRG workshops and final revisions to NEI 13-10 and NEI 08-09.

7) Section 4.11, *Roles and Responsibilities:* As stated above in, the CSIRT [Cyber Security Incident Response Team] will require SCANA resources from outside of VCSNS Unit 1. Once the interface agreements are issued this item will be satisfied.

Criteria 3 A proposed completion date for Milestone 8 consistent with the remaining scope of work to be conducted and the resources available.

In response to Criteria 3, the licensee provided that the remainder of the Milestone 8 work will be fully implemented by the proposed Milestone 8 completion date of December 31, 2017.

The licensee further stated:

> The additional time requested to complete Milestone 8 will not impact the over-all effectiveness of the cyber security program. With the completion of the cyber security Milestones 1 through 7 Inspection and the corrective actions associated with the inspection, there is no impact to safe and reliable power operation. The Milestone 8 extension will also provide time to fully integrate the cyber security plan into the station's programs, processes, procedures and training.

Criteria 4 An evaluation of the impact that the additional time to implement the requirements will have on the effectiveness of the licensee's overall cyber security program in the context of milestones already completed.

In response to Criteria 4, the licensee indicated VCSNS Unit 1 completed the implementation of interim milestones 1 thru 7 as documented in Inspection Report No. 05000395/2015407 (ADAMS Accession No. ML15355A394). The completed activities provide a high degree of protection against cyber attacks while VCSNS Unit 1 implements the full program. The licensee further provided details about the completed milestones and in-progress Milestone 8 activities.

Criteria 5 A description of the licensee's methodology for prioritizing completion of work for critical digital assets associated with significant safety consequences and with reactivity effects in the balance of plant.

In response to Criteria 5, the licensee stated:

> VCSNS Unit 1 CDA equipment listings are divided into approximately equal quantities of Security and Non-Security CDAs. This division of CDA lists makes it inherently more efficient to accomplish Security and non-Security CDA assessments in parallel. Non-Security assets are categorized as Safety, Important to Safety (Augmented Quality and BOP), Support, Connectivity and Emergency Preparedness which are prioritized in-that order. All assessments will begin with Type III assets. The methodology is based on defense-in-depth, installed configuration of the CDA and susceptibility to the five commonly identified threat vectors. Program procedures will be developed prior to the completion of the assessments and implementation will be addressed as part of the assessment mitigation activities. Significant vulnerabilities and threats that are discovered prior to full program implementation will be documented in the Corrective Action Program upon discovery. Work orders or Corrective Actions will be created to address mitigation. Prioritization will be based on Safety and Security significance of the mitigation activities. Other factors such as difficulty to implement and equipment availability (outage to support offline required work) will also factor into prioritization.

Criteria 6 A discussion of the licensee's cyber security program performance up to the date of the license amendment request.

In response to Criteria 6, the licensee stated:

> VCSNS Unit 1 completed the implementation of interim milestones 1 thru 7 as documented in Inspection Report No. 05000395/2015407. The completed activities address significant cyber attack vectors, which provide a high degree of protection against cyber attacks during implementation of the full program.

The licensee further include details regarding the completed activities.

Criteria 7 A discussion of cyber security issues pending in the licensee's corrective action program (CAP).

In response to Criteria 7, the licensee stated:

> VCSNS Unit 1 uses the site CAP to document all cyber issues in order to trend, correct, and improve the VCSNS Unit 1 Cyber Security Program. The CAP database documents and tracks from initiation through closure, all cyber security required actions including issues identified during on-going program assessment activities. Adverse trends are monitored for-program improvement and addressed via the CAP process.

The licensee further provided examples of issues and activities closed and pending in the VCSNS Unit 1 CAP.

Criteria 8 A discussion of modifications completed to support the cyber security program and a discussion of pending cyber security modifications.

In response to Criteria 8, the licensee provided a discussion of completed and pending modifications to support the cyber security program.

3.2 NRC Staff Evaluation

The NRC staff has evaluated the licensee's application using the regulatory requirements and the guidance set forth above. The NRC staff finds that the actions the licensee noted as being required to implement CSP, Section 3, "Analyzing Digital Computer Systems and Networks" and Section 4, "Establishing, Implementing and Maintaining the Cyber Security Program" are reasonable, as discussed below.

The licensee indicated VCSNS Unit 1 completed the implementation of interim Milestones 1 through 7. The completed activities provide a high degree of protection against cyber attacks to ensure that the most significant digital computer and communication systems and networks associated with SSEP functions are sufficiently protected against cyber attacks, while VCSNS Unit 1 implements the full program. The licensee further provided details about the completed milestones and in-progress Milestone 8 activities. On this basis, the NRC staff finds that the licensee's site is more secure after implementation of Milestones 1 through 7 at VCSNS Unit 1 because the activities that the licensee completed will mitigate the most significant cyber attack vectors for the most significant CDAs.

The licensee proposed a Milestone 8 completion date of December 31, 2017. The NRC staff has had extensive interaction with the nuclear industry since licensees first developed their CSP implementation schedules. The licensee stated that changing the completion date of Milestone 8 will allow for sufficient time to assess, plan, schedule, and implement any plant or programmatic changes resulting from the resolution of industry generic issues. Based on this interaction, the NRC staff recognizes that CDA assessment work is much more complex and resource-intensive than originally anticipated. As a result, the licensee has a large number of additional tasks not considered when developing its current CSP implementation schedule. The NRC staff concludes that the licensee's request for additional time to implement Milestone 8 is reasonable, given the effectiveness of the VCSNS Unit 1 CSP with Milestones 1 through 7 already in place, and the unanticipated complexity and scope of work required to come into full compliance with the current CSP.

VCSNS's prioritization and performance of work is based on safety significance, required availability of significant systems, and consideration for all aspects and elements of risk management. The NRC staff concludes that based on the large number of tasks described above and the limited resources with the appropriate expertise to perform these activities, the licensee's methodology for prioritizing work on CDAs is appropriate. The staff further concludes that the licensee's request to delay final implementation of the CSP until December 31, 2017, is reasonable given the complexity of the remaining unanticipated work.

The NRC staff further finds that the licensee's request to delay final implementation of the CSP until December 31, 2017, is reasonable. In reaching this finding, the staff considered: (1) pending cyber security modifications; (2) the status of the cyber security program; (3) the integration of cyber security into the station's programs, processes, procedures and training; and (4) outage related cyber security work will occur during the spring of 2017. Therefore, the NRC has reasonable assurance that full implementation of the CSP by December 31, 2017, will provide adequate protection of the public health and safety and the common defense and security.

3.3 NRC Staff Conclusion

The NRC staff concludes that the licensee's request to delay full implementation of its CSP until December 31, 2017, is reasonable for the following reasons: (i) the licensee's implementation of Milestones 1 through 7 provides mitigation for significant cyber attack vectors for the most significant CDAs as discussed above; (ii) the scope of the work required to come into full compliance with the CSP implementation schedule was more complicated and resource intensive than anticipated and not reasonably foreseeable; and (iii) the licensee has reasonably prioritized and scheduled the work required to come into full compliance with its CSP implementation schedule. The staff concludes that the licensee's request for additional time to implement Milestone 8 is reasonable, given the complexity, volume, and scope of the remaining work required to fully implement its CSP. The NRC has reasonable assurance that full implementation of the CSP by the proposed date of December 31, 2017, will provide adequate protection of the public health and safety and the common defense and security.

The NRC staff also concludes that, upon full implementation of the licensee's cyber security program, the requirements of the licensee's CSP and 10 CFR 73.54 will be met. Therefore, the NRC staff finds the proposed change acceptable.

4.0 STATE CONSULTATION

In accordance with the Commission's regulations, the South Carolina State official was notified of the proposed issuance of the amendment on January 27, 2017. The State official had no comments.

5.0 ENVIRONMENTAL CONSIDERATION

This amendment relates to modifications to systems used for security and thus meets the eligibility criteria for a categorical exclusion set forth in 10 CFR 51.22(c)(12)(ii). Pursuant to 10 CFR 51.22(b), no environmental impact statement or environmental assessment need be prepared in connection with the issuance of this amendment. The Commission has previously issued a proposed finding that the amendments involve no significant hazards consideration, and there has been no public comment on such finding published in the *Federal Register* on October 4, 2016 (81 FR 68472).

6.0 CONCLUSION

The Commission has concluded, based on the considerations discussed above, that: (1) there is reasonable assurance that the health and safety of the public will not be endangered by operation in the proposed manner, (2) there is reasonable assurance that such activities will be conducted in compliance with the Commission's regulations, and (3) the issuance of the amendments will not be inimical to the common defense and security or to the health and safety of the public.

Principal Contributor: John Rycyna, NRR

Date: March 9, 2017