



Thomas D. Gatlin  
Vice President, Nuclear Operations  
803.345.4342

August 5, 2010  
RC-10-0091

U. S. Nuclear Regulatory Commission  
Document Control Desk  
Washington, D.C. 20555

Attention: R. E. Martin

Dear Sir / Madam:

Subject: VIRGIL C. SUMMER NUCLEAR STATION (VCSNS) UNIT 1  
DOCKET NO. 50-395  
OPERATING LICENSE NO. NPF-12  
WITHDRAWAL AND RESUBMITTAL OF LICENSE AMENDMENT  
REQUEST TO FACILITY OPERATING LICENSE TO INCORPORATE  
THE REQUIREMENTS OF 10 CFR 73.54

Reference: Jeffery B. Archie, SCE&G, Letter (RC-09-0110) to the Document Control Desk, dated November 20, 2009, submitting License Amendment Request (LAR) to the Facility Operating License to Incorporate the Requirements of 10 CFR 73.54

In accordance with the provisions of 10 CFR 50.4 and 50.90, South Carolina Electric & Gas Company (SCE&G) is withdrawing the previously submitted request for an amendment to the Facility Operating License (FOL) for VCSNS Unit 1 dated November 20, 2009. Additionally, VCSNS Unit 1 is requesting the NRC simultaneously accept, for review, the enclosed request for an amendment to the FOL to replace the previously submitted request dated November 20, 2009.

The enclosed proposed amendment that requests NRC approval of the VCSNS Cyber Security Plan provides an implementation schedule and adds a sentence to the existing FOL Physical Protection license condition to require VCSNS fully implement and maintain in effect all provisions of the Commission approved Cyber Security Plan.

The enclosed proposed amendment conforms to the model application provided in the NRC endorsed (Office of Nuclear Security and Incident Response letter dated May 5, 2010, ADAMS Accession No. ML101190371), NEI 08-09 "Cyber Security Plan for Nuclear Power Reactors" Revision 6.

**Enclosure transmitted herewith contains ~~Security Related Information~~  
When separated from enclosure, this transmittal document is decontrolled.**

Stoia  
NLR

Document Control Desk  
CR-09-03585 / RC-10-0091  
Page 2 of 3

Enclosure 1 provides an evaluation of the proposed change. Enclosure 1 also contains the following attachments:

- Attachment 1 provides the existing FOL pages marked up to show the proposed change.
- Attachment 2 provides the proposed FOL change in final typed format.

Enclosure 2 provides a copy of the VCSNS Unit 1 High-Level Milestones Schedule for implementation of 10 CFR 73.54 requirements. The implementation schedule includes the following two parallel implementation paths:

- The Physical Protection path which deterministically isolates Level 3 and 4 Critical Digital Assets from external cyber attack.
- The Program Development and Implementation path.

Enclosure 2 also includes regulatory commitment dates (denoted with \*\*) and other milestones date that are for scheduling purposes but are not considered regulatory commitments. The last page of Enclosure 2 contains a separate table listing the regulatory commitment dates. SCE&G requests that Enclosure 2, which contains sensitive information, be withheld from public disclosure in accordance with 10 CFR 2.390.

Enclosure 3 provides a copy of the VCSNS Unit 1 Cyber Security Plan which is a standalone document that will be incorporated by reference into the VCSNS Physical Security Plan upon approval. SCE&G requests that Enclosure 3, which contains sensitive information, be withheld from public disclosure in accordance with 10 CFR 2.390.

Enclosure 4 provides a deviation table which includes a description of changes to the un-bracketed text of NEI 08-09, Revision 6.

Once approved, SCE&G requests a 60 sixty day period to make the page change to the FOL.

In accordance with 10 CFR 50.91, a copy of this application, with attachments, is being provided to the designated South Carolina Official.

If you should have any questions regarding this submittal, please contact Mr. Bruce L. Thompson at (803) 931-5042.

Document Control Desk  
CR-09-03585 / RC-10-0091  
Page 3 of 3

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

8/5/10 Executed on Tom Datt  
Thomas D. Gatlin

WH/TDG/dr

Enclosure 1 – Evaluation of Proposed Change  
Enclosure 2 – Cyber Security Plan Implementation Schedule  
Enclosure 3 – Virgil C. Summer Nuclear Station Unit 1 Cyber Security Plan  
Enclosure 4 – Virgil C. Summer Nuclear Station Unit 1 NEI 08-09 Rev. 6 Deviation Table

c: (without Enclosures unless noted)  
K. B. Marsh  
S. A. Byrnes  
J. B. Archie  
N. S. Carns  
J. H. Hamilton  
R. J. White  
W. M. Cherry  
L. A. Reyes (With Enclosures)  
R. E. Martin (With Enclosures)  
T. P. O’Kelley (With Enclosures)  
NRC Resident Inspector  
P. Ledbetter  
K. M. Sutton  
NSRC  
RTS (CR-09-03585)  
File (813.20)  
PRSF (RC-10-0091, With Enclosures)

Enclosure 1

Evaluation of Proposed Change  
Request for Approval of the  
Virgil C. Summer Nuclear Station Unit 1 Cyber Security Plan

- 1.0 Summary Description
  - 2.0 Detailed Description
  - 3.0 Technical Evaluation
  - 4.0 Regulatory Evaluation
  - 4.1 Applicable Regulatory Requirements / Criteria
  - 4.2 Significant Hazards Consideration
  - 5.0 Environmental Consideration
  - 6.0 References
- 

**ATTACHMENTS**

Attachment 1 - Marked FOL pages

Attachment 2 - FOL changes in final typed format.

### **1.0 SUMMARY DESCRIPTION**

The proposed license amendment request (LAR) includes the proposed Virgil C. Summer Nuclear Station (VCSNS) Unit 1 Cyber Security Plan, an Implementation Schedule, and a proposed sentence to be added to the existing FOL Physical Protection license condition.

### **2.0 DETAILED DESCRIPTION**

The proposed license amendment request (LAR) includes three parts: the proposed Plan, an Implementation Schedule, and a proposed sentence to be added to the existing FOL Physical Protection license condition to require South Carolina Electric & Gas Company (SCE&G) to fully implement and maintain in effect all provisions of the Commission approved cyber security plan as required by 10 CFR 73.54. Federal Register notice issued the final rule that amended 10 CFR Part 73. The regulations in 10 CFR 73.54, "Protection of digital computer and communication systems and networks," establish the requirements for a cyber security program. This regulation specifically requires each licensee currently licensed to operate a nuclear power plant under Part 50 of this chapter to submit a cyber security plan that satisfies the requirements of the Rule. Each submittal must include a proposed implementation schedule and implementation of the licensee's cyber security program must be consistent with the approved schedule. The background for this application is addressed by the NRC Notice of Availability published on March 27, 2009, 74 FR 13926 (Reference 1).

### **3.0 TECHNICAL EVALUATION**

Federal Register notice 74 FR 13926 issued the final rule that amended 10 CFR Part 73. Cyber security requirements are codified as new 73.54 and are designed 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 established by 73.1(a)(1)(v). These requirements are substantial improvements upon the requirements imposed by EA-02-026 (Reference 2).

NRC issued Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities" in January 2010 which provides an approach the NRC staff deems acceptable for complying with the Commission's regulations for protecting digital computers, communications systems, and networks. NEI 08-09, "Cyber Security Plan Template" has been endorsed by NRC letter (Office of Nuclear Security and Incident Response letter dated May 5, 2010, ADAMS Accession No. ML101190371) (Reference 3) for use by licensees in development of their own cyber security plans.

This LAR includes the proposed Plan (Enclosure 3) that conforms to the template provided in NEI 08-09 Rev. 6. In addition the LAR includes the proposed change to the existing FOL license condition for "Physical Protection" (Attachments 1 and 2 of this enclosure). Finally, the LAR contains the proposed Implementation Schedule (Enclosure 2) as required by 10 CFR 73.54,

## **4.0 REGULATORY EVALUATION**

### **4.1 APPLICABLE REGULATORY REQUIREMENTS / CRITERIA**

This LAR is submitted pursuant to 10 CFR 73.54 which requires licensees currently licensed to operate a nuclear power plant under 10 CFR Part 50 to submit a Cyber Security Plan as specified in 50.4 and 50.90.

### **4.2 SIGNIFICANT HAZARDS CONSIDERATION**

SCE&G has evaluated the proposed changes using the criteria in 10 CFR 50.92 and has determined that the proposed changes do not involve a significant hazards consideration. An analysis of the issue of no significant hazards consideration is presented below.

The proposed change incorporates a new requirement into the facility operating license to implement and maintain a cyber security plan. This new requirement is being included as part of an existing facility operating license condition that requires the implementation and maintenance of physical security, training and qualification, and safeguards contingency plans. The Cyber Security Plan describes how the requirements of 10 CFR 73.54 will be implemented in order to protect the health and safety of the public from radiological sabotage as a result of a cyber attack. The plan conforms to the template provided in NEI 08-09, Revision 6, with deviations, and provides a description of how the requirements of 10 CFR 73.54 will be implemented at VCSNS Unit 1. The Cyber Security Plan establishes the licensing basis for the Cyber Security Program for VCSNS Unit 1. The Cyber Security Plan establishes how to achieve high assurance that nuclear power plant digital computer and communication systems and networks associated with the following are adequately protected against cyber attacks up to and including the design basis threat:

1. Safety-related and important-to-safety functions,
2. Security functions,
3. Emergency preparedness functions including offsite communications, and
4. Support systems and equipment, which if compromised, would adversely impact safety, security, or emergency preparedness functions.

**Criterion 1: The proposed change does not involve a significant increase in the probability or consequences of an accident previously evaluated.**

The proposed change incorporates a new requirement, in the Operating License, to implement and maintain a cyber security plan as part of the facility's overall program for physical protection. The Cyber Security Plan itself does not require any plant modifications. Rather, the Cyber Security Plan describes how the requirements of 10 CFR 73.54 are implemented in order to identify, evaluate, and mitigate cyber attacks up to and including the design basis threat, thereby achieving high assurance that the facility's digital computer and communications systems and networks are protected from cyber attacks. The proposed change requiring the implementation and maintenance of a Cyber Security Plan does not alter the plant configuration, require new plant equipment to be installed, alter accident analysis assumptions, add any accident initiators, or affect the function of plant systems or the manner in which systems are operated, maintained, modified, tested, or inspected; therefore, the inclusion of the Cyber Security Plan as a part of the facility's other physical protection programs specified in the facility's operating license has no impact on the probability or consequences of an accident previously evaluated.

**Criterion 2: The proposed change does not create the possibility of a new or different kind of accident from any accident previously evaluated.**

The proposed change incorporates a new requirement, in the Operating License, to implement and maintain a cyber security plan as part of the facility's overall program for physical protection. The creation of the possibility of a new or different kind of accident requires creating one or more new accident precursors. New accident precursors may be created by modifications of the plant's configuration, including changes in the allowable modes of operation. The Cyber Security Plan itself does not require any plant modifications, nor does the Cyber Security Plan affect the control parameters governing unit operation or the response of plant equipment to a transient condition. Because the proposed change does not change or introduce any new equipment, modes of system operation, or failure mechanisms, no new accident precursors are created. Therefore, the proposed change does not create the possibility of a new or different kind of accident from any accident previously evaluated.

**Criterion 3: The proposed change does not involve a significant reduction in a margin of safety.**

The proposed change incorporates a new requirement, in the Operating License, to implement and maintain a cyber security plan as part of the facility's overall program for physical protection. Plant safety margins are established through Limiting Conditions for Operation, Limiting Safety System Settings, and Safety limits specified in the Technical Specifications. Because the Cyber Security Plan itself does not require any plant modifications and does not alter the operation of plant equipment, the proposed change

does not change established safety margins. Therefore, the proposed change does not involve a significant reduction in a margin of safety.

#### **4.3 CONCLUSION**

Based on the above, SCE&G concludes that the proposed change presents no significant hazards consideration under the standards set forth in 10 CFR 50.92(c), and accordingly, a finding of no significant hazards consideration is justified.

#### **5.0 ENVIRONMENTAL CONSIDERATION**

The proposed amendment establishes the licensing basis for a Cyber Security Program for VCSNS Unit 1 and will be a part of the Physical Security Plan. This proposed amendment will not involve any significant construction impacts. Pursuant to 10 CFR 51.22(c)(12) no environmental impact statement or environmental assessment need be prepared in connection with the issuance of the amendment.

#### **6.0 REFERENCES**

1. Federal Register Notice, Final Rule 10 CFR Part 73, Power Reactor Security Requirements, published on March 27, 2009, 74 FR 13926.
2. EA-02-026, Order Modifying Licenses, Safeguards and Security Plan Requirements, issued February 25, 2002.
3. Office of Nuclear Security and Incident Response letter dated May 5, 2010, ADAMS Accession No. ML101190371

Attachment 1  
Proposed Facility Operating License Change (Mark-Up)

-11a-

- 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 contains 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.

**INSERT THE FOLLOWING**

SCE&G shall fully implement and maintain in effect all provisions of the Commission-approved VCSNS Unit 1 cyber security plan submitted by letter dated August 5, 2010 and withheld from public disclosure in accordance with 10 CFR 2.390

Renewed Facility Operating License No. NPF-12  
~~Revised by letter dated October 28, 2004~~  
~~Revised by letter dated November 18, 2004~~  
~~Revised by letter dated January 20, 2007~~  
Revised by letter dated August 23, 2007

- 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 contains 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 VCSNS Unit 1 cyber security plan submitted by letter dated August 5, 2010 and withheld from public disclosure in accordance with 10 CFR 2.390.

Enclosure 4  
 Virgil C. Summer Nuclear Station Unit 1  
 NEI 08-09 Rev. 6 Deviation Table

#	NEI 08-09 Location	NEI 08-09 Rev 6 Text	Summer Text	Discussion
1	Appendix B, definition of Cyber Attack	Any event in which there is reason to believe that an adversary has committed or caused, or attempted to commit or cause, or has made a credible threat to commit or cause malicious exploitation of a SSEP function.	Any event in which there is reason to believe that an adversary has committed or caused, or attempted to commit or cause, or has made a credible threat to commit or cause malicious exploitation of a SSEP function <del>function</del> CDA.	This revision to the definition of Cyber Attack results from comments provided by NRC following their review of NEI 08-09, Rev 6. Reference letter from NEI Christopher E. Earls to NRC Richard P. Correia dated June 2, 2010.
2	Appendix A, section 3.1.2, sixth bullet, last phrase	<p>The roles and responsibilities of the CSAT include such activities as:</p> <ul style="list-style-type: none"> <li>Evaluating assumptions and conclusions about cyber security threats; potential vulnerabilities to, and consequences from an attack; the effectiveness of existing cyber security controls, defensive strategies, and attack mitigation methods; cyber security awareness and training of those working with, or responsible for CDAs and cyber security controls throughout their system life cycles; and estimates of cyber security risk</li> </ul>	<p>The roles and responsibilities of the CSAT include such activities as:</p> <ul style="list-style-type: none"> <li>Evaluating assumptions and conclusions about cyber security threats; potential vulnerabilities to, and consequences from an attack; the effectiveness of existing cyber security controls, defensive strategies, and attack mitigation methods; cyber security awareness and training of those working with, or responsible for CDAs and cyber security controls throughout their system life cycles. <del>and estimates of cyber security risk</del></li> </ul>	This deviation deletes the CSAT responsibility for estimating cyber security risk since there is no basis for performing this action (e.g., how to perform this function, when this is performed, or how the information is used). This bullet has been revised and now reads consistent with Reg Guide 5.71.

Enclosure 4  
Virgil C. Summer Nuclear Station Unit 1  
NEI 08-09 Rev. 6 Deviation Table

3	Appendix A Section 4.7	<ul style="list-style-type: none"><li>Procedures for operating the CDAs in manual mode with external electronic communications connections severed until secure conditions can be restored</li></ul>	<ul style="list-style-type: none"><li>Procedures for <b>severing external electronic communications connections, where allowed</b> operating the CDAs in manual mode with external electronic communications connections severed, until secure conditions can be restored</li></ul>	Deleted "operating the CDAs in manual mode" based on its conflict with the Technical Specification Limiting Conditions for Operation as defined under 10 CFR 50.36. There may be conditions and CDAs in a nuclear power plant that are not permitted to be operated in manual mode with external communication connections severed. This deviations revise the requirement to sever the communication connections where allowed and deletes the requirement to operate the CDA in a manual mode.
---	---------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Enclosure 4  
Virgil C. Summer Nuclear Station Unit 1  
NEI 08-09 Rev. 6 Deviation Table

4	Appendix A, section 3.1.4, first paragraph	The CSAT collects, examines, and documents the existing cyber security policies, procedures, and practices; existing cyber security controls; detailed descriptions of network and communication architectures (or network/communication architecture drawings); information on security devices; and any other information that may be helpful during the cyber security assessment process. The team collects, documents by reference and evaluates the following as they apply to CDAs:	The CSAT collects, examines, and documents the existing cyber security policies, procedures, and practices; existing cyber security controls; detailed descriptions of network and communication architectures (or network/communication architecture drawings); information on security devices; and any other information that may be helpful during the cyber security assessment process. The team collects, documents by reference and <del>evaluates</del> <b>examines</b> the following as they apply to CDAs:	The word "evaluates" has been replaced by "examines" to be consistent with both the Title of the section and other uses of the word in the section. It is clear that there is no additional evaluation implied with this requirement and the text should be revised to read "examine" to avoid unintended meaning.
---	--------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Enclosure 4  
Virgil C. Summer Nuclear Station Unit 1  
NEI 08-09 Rev. 6 Deviation Table

5	Appendix D, Control 2.5, 4 <sup>th</sup> Bullet, 3 <sup>rd</sup> sub-bullet	○ Ensures CDAs with auditing failures take the following additional actions: 1. Shut down the CDA,	○ Ensures CDAs with auditing failures take the following additional actions: 1. Shut down the <b>CDA (if appropriate)</b> ,	Appendix D, Control 2.5 discusses "Response To Audit Processing Failures". The Control states that CDAs should be shut down when auditing failures occur. Depending on the function of the CDA in a nuclear power plant, it may not be possible in all circumstances to shut down a CDA. The control is being revised to acknowledge the CDA may not be able to be immediately shut down.
---	-----------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Enclosure 4  
 Virgil C. Summer Nuclear Station Unit 1  
 NEI 08-09 Rev. 6 Deviation Table

6	Appendix D, Control 1.4, 6 <sup>th</sup> and 7 <sup>th</sup> Bullets,	<p>1.4 Information Flow Enforcement</p> <p>This Technical cyber security control:</p> <ul style="list-style-type: none"> <li>• Implements one-way data flows using hardware mechanisms, implementing dynamic information flow control based on policy that allows or disallows information flows based on changing conditions or operational considerations.</li> <li>• Implements information flow control enforcement using dynamic security policy mechanisms as a basis for flow control decisions.</li> </ul>	<p>1.4 Information Flow Enforcement</p> <p>This Technical cyber security control:</p> <ul style="list-style-type: none"> <li>• <b>For Deterministic devices:</b> Implements one-way data flows using hardware mechanisms, <del>implementing dynamic information flow control based on policy that allows or disallows information flows based on changing conditions or operational considerations.</del></li> <li>• <b>For Non-deterministic devices:</b> Implements information flow control enforcement using dynamic security policy mechanisms as a basis for flow control decisions.</li> </ul>	<p>The two bulleted controls have are being revised to remove ambiguity in how they are applied to both non-deterministic firewalls and deterministic data diodes. Both types of devices are being implemented as part of Summer's defensive architecture.</p>
---	-----------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Enclosure 4  
 Virgil C. Summer Nuclear Station Unit 1  
 NEI 08-09 Rev. 6 Deviation Table

<p>7</p>	<p>Appendix E, Section 6, 4th bullet.</p> <p>Next to last bullet</p>	<p>This security control implements and documents a defensive strategy that:</p> <ul style="list-style-type: none"> <li>• Allows only one-way direct data flow from higher security levels to lower security levels.</li> </ul> <p>In addition, this security control implements and documents security boundary control devices between higher security levels and lower security levels that:</p> <ul style="list-style-type: none"> <li>○ Except in the case of data diodes, contain a rule set that at a minimum       <ul style="list-style-type: none"> <li>▪ Allows no information of any kind, including handshaking protocols, to be transferred directly from networks or systems existing at the lower security level to networks or systems existing at the higher security level;</li> </ul> </li> </ul>	<p>This security control implements and documents a defensive strategy that:</p> <ul style="list-style-type: none"> <li>• <b>For deterministic devices (e.g., data diodes),</b> allows only one-way direct data flow from higher security levels to lower security levels.</li> </ul> <p>In addition, this security control implements and documents security boundary control devices between higher security levels and lower security levels that:</p> <ul style="list-style-type: none"> <li>○ Except in the case of data diodes, contain a rule set that at a minimum       <ul style="list-style-type: none"> <li>• <del>Allows no information of any kind, including handshaking protocols, to be transferred directly from networks or systems existing at the lower security level to networks or systems existing at the higher security level;</del></li> </ul> </li> </ul>	<p>For Summer, the boundary between Level 3 and Level 2 is implemented by one or more deterministic devices (i.e., data diodes, air gaps) that isolate CDAs in or above level 3. The boundary between level 4 and level 3 is implemented by either one or more deterministic devices (i.e., data diodes, air gaps) that isolate CDAs in level 4, or one or more non-deterministic network isolation devices. Information flows between level 3 and 4 are restricted through the use of a firewall and network-based intrusion detection system.</p> <p>The first revised bullet discusses the restriction to one-way communication between levels. Summer's defensive architecture allows use of a firewall within the boundary of a deterministic device (i.e., level 3 to level 4) which under controlled conditions may allow some transfer of information from lower to higher level.</p> <p>The second revised bullet is deleted. This bullet discusses boundary devices other than diodes (e.g., firewalls). The</p>
----------	----------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Enclosure 4  
 Virgil C. Summer Nuclear Station Unit 1  
 NEI 08-09 Rev. 6 Deviation Table

				restriction of no data transfer is removed and not necessary in Summer's architecture which employs a data diode or air gap between level 2 and level 3.
8	Appendix E Control 7.1, last paragraph	<p>Stakeholders are included in the development of incident response policies, procedures and plans, including the following groups:</p> <ul style="list-style-type: none"> <li>• Physical security</li> <li>• Cyber security team</li> <li>• Operations</li> <li>• Engineering</li> <li>• Information Technology</li> <li>• Human resources</li> <li>• System support vendors</li> <li>• Management</li> <li>• Legal</li> <li>• Safety</li> </ul>	<p>Stakeholders are included in the development of incident response policies, procedures and plans. <del>including the following groups</del> For example:</p> <ul style="list-style-type: none"> <li>• Physical security</li> <li>• Cyber security team</li> <li>• Operations</li> <li>• Engineering</li> <li>• Information Technology</li> <li>• Human resources</li> <li>• System support vendors</li> <li>• Management</li> <li>• Legal</li> <li>• Safety</li> </ul>	<p>Appendix E, Control 7.1 is revised to recognize that all groups listed in the control are provided for example and not necessarily all required for the development of the incident response policies, procedures and plans.</p>