# 13.0 CONDUCT OF OPERATIONS

## 13.1 Organizational Structure of Applicant

### 13.1.1 Introduction

The organizational structure includes the design, construction, and preoperational responsibilities of the organizational structure. The management and technical support organization includes a description of the corporate or home office organization, its functions and responsibilities, the number and the qualifications of personnel. Its activities include facility design, design review, design approval, construction management, testing, and operation of the plant. The descriptions of the design and construction and preoperational responsibilities include the following:

- how these responsibilities are assigned by the headquarters staff and implemented within the organizational units
- the responsible working- or performance-level organizational unit
- the estimated number of persons to be assigned to each unit with responsibility for the project
- the general educational and experience requirements for identified positions or classes of positions
- early plans for providing technical support for the operation of the facility

This section also describes the structure, functions, and responsibilities of the onsite organization established to operate and maintain the plant.

### 13.1.2 Summary of Application

Section 13.1 of the V.C. Summer Nuclear Station (VCSNS) combined license (COL) Final Safety Analysis Report (FSAR), Revision 2, incorporates by reference Section 13.1 of the AP1000 Design Control Document (DCD), Revision 17.

In addition, in VCSNS COL FSAR Section 13.1, the applicant provided the following:

*AP1000 COL Information Items*

- VCS COL 13.1-1

The applicant provided additional information in VCS COL 13.1-1 to resolve COL Information Item 13.1-1 (COL Action Item 13.1-1). COL Information Item 13.1-1 requires the COL applicant to describe its organizational structure. VCS COL 13.1-1 describes organizational positions of the nuclear power station and owner/applicant corporations and associated functions and responsibilities.

- VCS COL 9.5-1

The applicant provided additional information in VCS COL 9.5-1, describing the fire protection program in Section 9.5.1.8. For this VCSNS COL item, the applicant added a new Section 13.1.1.2.10, “Fire Protection,” and a new Section 13.1.1.3.2.1.4, "Engineer in Charge of Fire Protection." Table 1.8-202, “COL Item Tabulation,” provides VCS COL 9.5-1 cross-references.

- VCS COL 18.6-1

The applicant provided additional information in VCS COL 18.6-1, describing the qualifications of the nuclear plant technical support personnel. VCS COL 18.6-1 is addressed under Section 13.1.1.4, “Qualifications of Technical Support Personnel,” and Section 13.1.3.1, “Qualification Requirements.” Table 1.8-202, “COL Item Tabulation,” provides VCS COL 18.6-1 cross-references.

- VCS COL 18.10-1

The applicant provided additional information in VCS COL 18.10-1 to address the responsibilities of the manager in charge of nuclear training. VCS COL 18.10-1 is addressed in Section 13.1.1.3.2.2.1, “Functional Manager in Charge of Training (Nuclear Training).” Table 1.8-202, “COL Item Tabulation,” provides VCS COL 18.10-1 cross-references.

### 13.1.3 Regulatory Basis

The regulatory basis of the information incorporated by reference is addressed in NUREG-1793, “Final Safety Evaluation Report [FSER] Related to Certification of the AP1000 Standard Design,” and its supplements.

In addition, the acceptance criteria associated with the relevant requirements of the Commission regulations for VCS COL 13.1-1, VCS COL 9.5-1, VCS COL 18.6-1, and VCS COL 18.10-1 are given in Sections 13.1.1, “Management and Technical Support Organization,” and 13.1.2-13.1.3, “Operating Organization,” of NUREG-0800, “Standard Review Plan [SRP] for the Review of Safety Analysis Reports for Nuclear Power Plants.”

The applicable regulatory guidance for the organizational structure of the applicant is as follows:

- American National Standards Institute (ANSI)/American Nuclear Society (ANS)-3.1-1993, as endorsed and amended by Regulatory Guide (RG) 1.8, Revision 3, “Qualification and Training of Personnel for Nuclear Power Plants.”

The applicable regulations and regulatory guidance for the management, technical support, and operating organizations of the applicant are as follows:

- Title 10 of the *Code of Federal Regulations* (10 CFR) 50.40, "Common standards"
- 10 CFR 50.54, "Conditions of licenses"
- RG 1.33, Revision 2, "Quality Assurance Program Requirements (Operation)"

### 13.1.4 Technical Evaluation

The Nuclear Regulatory Commission (NRC) staff reviewed Section 13.1 of the VCSNS COL FSAR and checked the referenced DCD to ensure that the combination of the DCD and the COL application represents the complete scope of information relating to this review topic.[1] The NRC staff's review confirmed that the information in the application and incorporated by reference addresses the required information relating to the organizational structure of the applicant. The results of the NRC staff's evaluation of the information incorporated by reference in the VCSNS COL application are documented in NUREG-1793 and its supplements.

The staff reviewed the information in the VCSNS COL FSAR:

*AP1000 COL Information Items*

- VCS COL 13.1-1

The NRC staff reviewed VCS COL 13.1-1 related to the organizational structure of the COL applicant included under Section 13.1 of the VCSNS COL FSAR. Section 13.1 of the VCSNS COL FSAR describes the organizational positions of a nuclear power plant and owner/applicant corporations and associated functions and responsibilities.

The applicant provided the following additional VCSNS site-specific COL information to resolve COL Information Item 13.1-1, which addresses the organizational structure of the COL applicant. COL Information Item 13.1-1 states:

> Combined License applicants referencing the AP1000 certified design will address adequacy of the organizational structure.

The commitment was also captured as COL Action Item 13.1-1 in Appendix F of NUREG-1793, which states:

> The COL applicant will describe its organizational structure.

The applicant provided additional information as part of the VCSNS COL FSAR to describe the organizational positions of a nuclear power station and owner/applicant corporations and associated functions and responsibilities. The position titles used in the text are generic and describe the function of the position. The applicant stated that VCSNS COL FSAR

[1] See Section 1.2.2 for a discussion of the staff's review related to verification of the scope of information to be included in a COL application that references a design certification (DC).

Table 13.1-201, “Generic Position/Site-Specific Position Cross-Reference” provides a cross-reference to identify site-specific position titles.

The applicant added new sections and information related to the site-specific organizational structure to VCSNS COL FSAR Section 13.1 beyond the structure given in RG 1.206, “Combined License Applications for Nuclear Power Plants (LWR [light-water reactor] Edition).” The new section titles are:

13.1.1, “Management and Technical Support Organization”
13.1.2, “Operating Organization”
13.1.3, “Qualifications of Nuclear Plant Personnel”
Table 13.1-201, “Generic Position/Site-Specific Position Cross-Reference”
Table 13.1-202, “Minimum On-Duty Operations Shift Organization for Two-Unit Plant”

In addition, the applicant added a new appendix to Chapter 13 titled “Appendix 13AA Construction-Related Organization.” This appendix describes the applicant’s construction organization. Once plant operation commences, this appendix will become historical information.

The NRC staff has reviewed VCS COL 13.1-1 and concludes that the management, technical support, and operating organizations, as described, are acceptable and meet the requirements of 10 CFR 50.40(b) based on the following.

The applicant has described its organization for the management of, and its means of providing, technical support for the plant staff for the design, construction, and operation of the facility and has described its plans for managing the project and utilizing the nuclear steam system supplier (NSSS) vendor and architect-engineer (AE). These plans provide reasonable assurance that the applicant will establish an acceptable organization and that sufficient resources are available to provide offsite technical support and to satisfy the applicant's commitments for the design, construction, and operation of the facility.

The applicant has described the assignment of plant operating responsibilities; the reporting chain up through the chief executive officer; the functions and responsibilities of each major plant staff group; the proposed shift crew complement for single-unit or multiple-unit operation; the qualification requirements for members of its plant staff; and staff qualifications. In Table 1.9-202, “Conformance with SRP Acceptance Criteria,” of the VCSNS COL FSAR, the applicant noted an exception to the criteria of NUREG-0800, Section 13.1.2-13.1.3 that suggests resumes of personnel holding plant managerial and supervisory positions be included in the FSAR. The staff finds this exception to the criteria of NUREG-0800, Section 13.1.2-13.1.3 acceptable because resumes for management and principal supervisory and technical positions will be available for review after position vacancies are filled.

NUREG-0800, Section 13.1.2-13.1.3, “Operating Organization,” provides the following acceptable characteristics for an applicant's operating organization:

1. The applicant is technically qualified, as specified in 10 CFR 50.40(b).

2. An adequate number of licensed operators will be available at all required times to satisfy the minimum staffing requirements of 10 CFR 50.54(j).

3. On-shift personnel are able to provide initial facility response in the event of an emergency.

4. Organizational requirements for the plant manager and radiation protection manager have been satisfied.

5. Qualification requirements and qualifications of plant personnel conform to the guidance of RG 1.8.

6. Organizational requirements conform to the guidance of RG 1.33.

The NRC staff finds that the operating organization proposed by the applicant will comply with these characteristics. These findings contribute to the judgment that the applicant complies with the requirements of 10 CFR 50.40(b). That is, the applicant is technically qualified to engage in design and construction activities and to operate a nuclear power plant; that the applicant will have the necessary managerial and technical resources to support the plant staff in the event of an emergency; and that the applicant has identified the organizational positions responsible for fire protection matters and delegated the authorities to these positions to implement fire protection requirements.

- VCS COL 9.5-1

The applicant added text to VCSNS COL FSAR Section 13.1.1.2.10, “Fire Protection,” indicating that the nuclear power station is committed to maintaining a fire protection program as described in VCSNS COL FSAR Section 9.5, and that the site vice president, through the engineer in charge of fire protection, is responsible for the fire protection program. The applicant added text to VCSNS COL FSAR Section 13.1.1.3.2.1.4, “Engineer in Charge of Fire Protection,” describing the responsibilities of the engineer in charge of the fire protection program.

The NRC staff reviewed VCS COL 9.5-1 relative to the text added to Sections 13.1.1.2.10 and 13.1.1.3.2.1.4 of the VCSNS COL application. Based on the management descriptions provided in Sections 13.1.1.2.10 and 13.1.1.3.2.1.4, the staff finds the applicant’s fire protection organization meets the guidance of NUREG-0800. The technical review for VCS COL 9.5-1 as it relates to the programmatic requirements is addressed in Section 9.5 of this safety evaluation report (SER).

- VCS COL 18.6-1

The NRC staff reviewed VCS COL 18.6-1, which describes the qualifications of the nuclear plant technical support personnel.

In Table 1.9-202, "Conformance with SRP Acceptance Criteria," of the VCSNS COL FSAR, the applicant noted an exception to the criteria of NUREG-0800, Section 13.1.1 that suggests the experience requirements of managers and supervisors of the technical support organization are included in the FSAR. The staff finds this exception to the criteria of NUREG-0800, Section 13.1.1 acceptable because the applicant added text to VCSNS COL FSAR Section 13.1.1.4, "Qualifications of Technical Support Personnel," stating the qualifications of managers and supervisors of the technical support organization will meet the education and experience requirements described in ANSI/ANS-3.1-1993 and RG 1.8.

The applicant added text to VCSNS COL FSAR Section 13.1.3, "Qualification Requirements," stating, in Section 13.1.3.1, the qualifications of managers, supervisors, operators, and technicians of the operating organization will meet the education and experience requirements described in ANSI/ANS-3.1-1993 and RG 1.8. In addition, Section 13.1.3.2 states that resumes and other documentation of the qualifications and experience of initial appointees to appropriate management and supervisory positions will be available for review after position vacancies are filled.

The applicant added VCSNS COL FSAR Table 13.1-202, "Minimum On-Duty Operations Shift Organization for Two-Unit Plant." Table 13.1-202 describes the minimum composition of the operating shift crew for all modes of operation. Position titles, license requirements and minimum shift manning for the various modes of operation are addressed in Technical Specifications and will be addressed in administrative procedures.

The NRC staff reviewed the text added to VCSNS COL FSAR Sections 13.1.1.4 and 13.1.3.1 relative to VCS COL 18.6-1 and concludes that the qualification requirements are acceptable and meet the requirements of 10 CFR 50.40(b) based on the following.

The applicant has described its organization for the management of, and its means of providing, technical support for the plant staff for the design, construction, and operation of the facility and has described its plans for managing the project and utilizing the NSSS vendor and AE. These plans give reasonable assurance that the applicant will establish an acceptable organization and that sufficient resources are available to provide offsite technical support and to satisfy the applicant's commitments for the design, construction, and operation of the facility.

- VCS COL 18.10-1

The NRC staff reviewed VCS COL 18.10-1 included under Section 13.1.1.3.2.2.1, "Functional Manager in Charge of Training (Nuclear Training)." This section describes the responsibilities of the manager in charge of nuclear training relative to the site training programs required for the safe and proper operation and maintenance of the plant. This item is cross-referenced to VCSNS COL FSAR Section 18.10 in Table 1.8-202, "COL Item Tabulation." The NRC staff concludes that the qualification requirements are acceptable and meet the requirements of

10 CFR 50.40(b) and the regulatory guidelines in NUREG-0800, Sections 13.1.1 and 13.1.2-13.1.3 because the applicant described how the training manager will carry out his or her position responsibilities for designing, developing, implementing, and maintaining training programs for the safe and proper operation and maintenance of the plant.

### 13.1.5 Post Combined License Activities

There are no post-COL activities related to this section.

### 13.1.6 Conclusion

The NRC staff reviewed the application and checked the referenced DCD. The NRC staff's review confirmed that the applicant addressed the required information relating to the organizational structure of the applicant, and there is no outstanding information expected to be addressed in the VCSNS COL FSAR related to this section. The results of the NRC staff's technical evaluation of the information incorporated by reference in the VCSNS COL application are documented in NUREG-1793 and its supplements.

In addition, the staff concludes that the information presented in the VCSNS COL FSAR is acceptable because it meets the acceptance criteria provided in NUREG-0800, Section 13.1. The staff based its conclusion on the following:

- VCS COL 13.1-1, related to the organizational structure of the COL applicant, is acceptable because it meets the requirements of 10 CFR 50.40(b).

- VCS COL 9.5-1, related to the fire protection organization meets the guidance of Section 13.1 of NUREG-0800 and is acceptable.

- VCS COL 18.6-1, related to the qualifications of nuclear plant technical support personnel, is acceptable because it meets the requirements of 10 CFR 50.40(b).

- VCS COL 18.10-1, related to the qualification requirements for the manager in charge of nuclear training, is acceptable because it meets the requirements of 10 CFR 50.40(b).

## 13.2 Training

### 13.2.1 Introduction

This section addresses the description and schedule of the training program for reactor operators (ROs) and senior reactor operators (SROs), i.e., licensed operators. It addresses the scope of licensing examinations as well as training requirements. The licensed operator training program also includes the requalification programs as required in 10 CFR 50.54(i)(i-1) and 10 CFR 55.59, "Requalification." In addition, this section of the VCSNS COL FSAR includes the description and schedule of the training program for non-licensed plant staff.

### 13.2.2 Summary of Application

Section 13.2 of the VCSNS COL FSAR, Revision 2, incorporates by reference Section 13.2 of the AP1000 DCD, Revision 17.

In addition, in VCSNS COL FSAR Section 13.2, the applicant provides the following:

*AP1000 COL Information Items*

- STD COL 13.2-1

The applicant provided additional information in Standard (STD) COL 13.2-1 to resolve COL Information Item 13.2-1 (COL Action Item 13.2-1), which incorporates the provisions of Nuclear Energy Institute (NEI) 06-13A, "Template for an Industry Training Program," providing the description and scheduling of the training program for plant personnel, including the requalification program for licensed operators.

- STD COL 18.10-1

The applicant provided additional information in STD COL 18.10-1 to address training for those operators involved in the Human Factors Engineering (HFE) Verification and Validation Program, using a systematic approach to training and Westinghouse Commercial Atomic Power (WCAP)-14655, "Designer's Input to the Training of the Human Factors Engineering Verification and Validation Personnel."

*License Conditions*

- Part 10, License Condition 3, Items B.1, C.3

The applicant proposed a license condition in Part 10 of the VCSNS COL application, which provides the milestones for implementing the Reactor Operator Training (B.1) and the applicable portions of the Non-Licensed Plant Staff Training Program (C.3) related to radioactive material. The license condition related to the portions of the Non-Licensed Plant Staff Training Program applicable to radioactive material is addressed in Chapter 1 of this SER.

- Part 10, License Condition 6

The applicant proposed a license condition to provide a schedule to support the NRC's inspection of operational programs included in VCSNS COL FSAR Table 13.4-201, including the Non-Licensed Plant Staff Training Program, Reactor Operator Training Program, and the Reactor Operator Requalification Program.

### 13.2.3 Regulatory Basis

The regulatory basis of the information incorporated by reference is addressed in NUREG-1793 and its supplements.

In addition, the acceptance criteria associated with the relevant requirements of the Commission regulations for the description and schedule of the training program for licensed operators are given in Sections 13.2.1 and 13.2.2 and Chapter 18 of NUREG-0800.

The applicable regulations and regulatory guidance documents for STD COL 13.2-1 are as follows:

- 10 CFR 50.54(m)
- 10 CFR Part 55, “Operators’ licenses”
- RG 1.8
- RG 1.149, “Nuclear Power Plant Simulation Facilities for Use in Operator Training and License Examinations”
- NUREG-1021, “Operator Licensing Examination Standards for Power Reactors”

The applicable regulations for the Non-Licensed Plant Staff Training Program are as follows:

- 10 CFR 50.120, “Training and qualification of nuclear power plant personnel”
- 10 CFR 52.79(a)(33), “Contents of applications; technical information”

The applicable regulations for the licensed operators training program are as follows:

- 10 CFR 55.13, “General exemptions”
- 10 CFR 55.31, “How to apply”
- 10 CFR 55.41, “Written examinations: Operators”
- 10 CFR 55.43, “Written examinations: Senior operators”
- 10 CFR 55.45, “Operating tests”

The applicable regulations for the licensed operator’s requalification program are found in:

- 10 CFR 50.34(b), “Final safety analysis report”
- 10 CFR 50.54(i)
- 10 CFR 55.59, “Requalification”

The applicable regulatory guidance for STD COL 18.10-1 is as follows:

- NUREG-0711, “Human Factors Engineering Program Review Model”

### 13.2.4 Technical Evaluation

The NRC staff reviewed Section 13.2 of the VCSNS COL FSAR and checked the referenced DCD to ensure that the combination of the DCD and the COL application represents the complete scope of information relating to this review topic.[1] The NRC staff’s review confirmed

that the information in the application and incorporated by reference addresses the required information relating to the description and schedule of the training programs for nuclear plant personnel. The results of the NRC staff's evaluation of the information incorporated by reference in the VCSNS COL application are documented in NUREG-1793 and its supplements.

Section 1.2.3 of this SER provides a discussion of the strategy used by the NRC to perform one technical review for each standard issue outside the scope of the DC and use this review in evaluating subsequent COL applications. To ensure that the staff's findings on standard content that were documented in the SER for the reference COL application (Vogtle Electric Generating Plant (VEGP), Units 3 and 4) were equally applicable to the VCSNS Units 2 and 3 COL application, the staff undertook the following reviews:

- The staff compared the VEGP COL FSAR, Revision 2 to the VCSNS COL FSAR. In performing this comparison, the staff considered changes made to the VCSNS COL FSAR (and other parts of the COL application, as applicable) resulting from requests for additional information (RAIs).

- The staff confirmed that all responses to RAIs identified in the corresponding standard content evaluation were endorsed.

- The staff verified that the site-specific differences were not relevant.

The staff has completed its review and found the evaluation performed for the standard content to be directly applicable to the VCSNS COL application. This standard content material is identified in this SER by use of italicized, double-indented formatting. Section 1.2.3 of this SER provides an explanation of why the standard content material from the SER for the reference COL application (VEGP) includes evaluation material from the SER for the Bellefonte Nuclear Plant (BLN) Units 3 and 4 COL application.

The following portion of this technical evaluation section is reproduced from Section 13.2.4 of the VEGP SER:

*AP1000 COL Information Items*

- *STD COL 13.2-1*

*The NRC staff reviewed STD COL 13.2-1 related to COL Information Item 13.2-1 (COL Action Item 13.2-1) included under Section 13.2 of the BLN COL FSAR. COL Information Item 13.2-1 states:*

> *The Combined License applicants referencing the AP1000 certified design will develop and implement training programs for plant personnel. This includes the training program for the operations personnel who participate as subjects in the human factors engineering verification and validation. These Combined License applicant training programs will address the scope of licensing examinations as well as new training requirements.*

*The commitment was also captured as COL Action Item 13.2-1 in Appendix F of the NRC staff FSER for the AP1000 DCD (NUREG-1793), which states:*

> *The COL applicant will develop and implement training programs for plant personnel.*

*The applicant provided the following text to supplement Section 13.2, "Training," of the AP1000 DCD, dealing with the training program for plant personnel.*

> *This section incorporates by reference NEI 06-13* (sic) [NEI 06-13A]*, Technical Report on a Template for an Industry Training Program Description. See Table 1.6-201.*

*This technical report provides a complete training program description for use with COL applications. The staff has endorsed NEI 06-13A, Revision 1, as it provides an acceptable template for describing licensed operators and non-licensed plant staff training programs. The applicant has incorporated by reference NEI 06-13A, Revision 1.*

*The applicant provided the following text to supplement Section 13.2, "Training," of the AP1000 DCD, which is included in the* [design certification] *DC amendment as part of the BLN COL FSAR to address STD COL 13.2-1, dealing with the training program for plant personnel.*

> *Table 13.4-201 provides milestones for training implementation.*

*NUREG-0800, Section 13.2.1, establishes milestones for the licensed operators and non-licensed plant staff training programs and for the licensed operator requalification training program. The BLN COL FSAR has identified those milestones in Table 13.4-201. The staff determined that this is acceptable, as the milestone information included in this table meets the criteria found in NUREG-0800.*

- *STD COL 18.10-1*

*The NRC staff reviewed STD COL 18.10-1, related to COL Information Item 18.10-1 (COL Action Item 18.10.3-1). COL Information Item 18.10-1 states:*

> *Combined License applicants referencing the AP1000 certified design will develop and implement training programs for plant personnel. This includes the training program for the operations personnel who participate as subjects in the human factors engineering verification and validation. These Combined License applicant training programs will address the scope of licensing examinations as well as new training requirements.*

*The commitment was also captured as COL Action Item 18.10.3-1 in Appendix F of the NRC staff's FSER for the AP1000 DCD (NUREG-1793), which states:*

> *With regard to the training program development, the COL applicant will: (1) address the training program development considerations in NUREG-0711, (2) address relevant concerns identified in this report* [NUREG-1793], *and (3) identify the minimum documentation that the COL applicant will provide to enable the staff to complete its review.*

*This section refers to Sections 13.1, "Organizational Structure of Applicant" and 13.2, "Training" regarding the training program development.*

*The NRC staff reviewed the resolution to STD COL 18.10-1, related to staffing and qualifications included under Section 18.10 of the BLN COL FSAR. The applicant provided the referenced NRC-endorsed NEI 06-13A, Revision 1, to address COL Information Item 18.10-1.*

*NEI 06-13A, Revision 1 was written to provide COL applicants with a generic program description for use with COL application submittals. In a letter dated December 5, 2008, the staff stated that the training template of NEI 06-13A, Revision 1, was an acceptable means for describing licensed operator and non-licensed plant staff training programs. The staff finds the applicant's incorporation of NEI 06-13A, Revision 1 to be acceptable because it utilizes an NRC-endorsed methodology.*

*In Table 1.9-202, "Conformance with SRP Acceptance Criteria," of the BLN COL FSAR, the applicant identified two exceptions to the criteria of NUREG-0800, Section 13.2, which recommends following the guidance in NUREG-0711 and RG 1.149. Further, the applicant stated in Table 1.9-202 that NEI 06-13A is incorporated by reference into the BLN COL FSAR. The staff's safety evaluation report for NEI 06-13A (ML0709504790) states that NEI 06-13A complies with the guidance in NUREG-0711 and RG 1.149. Therefore, the staff finds the two exceptions to the criteria in NUREG-0800, Section 13.2 to be acceptable because NEI 06-13A complies with the guidance in NUREG-0711 and RG 1.149.*

*<u>License Conditions</u>*

- *Part 10, License Condition 3, Item B1*

*The NRC staff finds the implementation milestone for the Reactor Operator Training Program (18 months prior to schedule date of initial fuel load) to be acceptable because it is consistent with 10 CFR 50.54(m).*

- *Part 10, License Condition 6*

*The applicant proposed a license condition in Part 10 of the VEGP COL application to provide a schedule to support the NRC's inspection of operational programs, including the Non-Licensed Plant Staff Training Program, Reactor Operator Training Program, and Reactor Operation Requalification Program. The proposed license condition is consistent with the policy established in SECY-05-0197 for operational programs in general, and is acceptable.*

### 13.2.5 Post Combined License Activities

For the reasons discussed in the technical evaluation section above, the staff proposes to include the following license conditions:

- License Condition (13-1) – The licensee shall implement the Reactor Operator Training Program at least 18 months prior to schedule date of initial fuel load.

- License Condition (13-2) – The licensee shall submit to the Director of NRO, a schedule, no later than 12 months after issuance of the COL, that supports planning for and conduct of NRC inspection of the operational program (the Non-Licensed Plant Staff Training Program, Reactor Operator Training Program, and Reactor Operation Requalification Program). The schedule shall be updated every 6 months until 12 months before scheduled fuel load, and every month thereafter until these operational programs have been fully implemented or the plant has been placed in commercial service, whichever comes first.

### 13.2.6 Conclusion

The NRC staff reviewed the application and checked the referenced DCD. The NRC staff's review confirmed that the applicant addressed the required information relating to the description and schedule of the training program for licensed operators, and there is no outstanding information expected to be addressed in the VCSNS COL FSAR related to this section. The results of the NRC staff's technical evaluation of the information incorporated by reference in the VCSNS COL application are documented in NUREG-1793 and its supplements.

In addition, the staff concludes that the information presented in the VCSNS COL FSAR is acceptable because it meets the acceptance criteria provided in NUREG-0800 Section 13.2. The staff based its conclusion on the following:

- STD COL 13.2-1 incorporates by reference NEI 06-13A, Revision 1, which provides an acceptable template for describing licensed operators and non-licensed plant staff training programs. The staff determined that this is acceptable, as it applies an NRC-endorsed approach.

- STD COL 18.10-1, relating to training, references Section 13.2 of the VCSNS COL FSAR, in which the applicant has committed to use WCAP-14655 to ensure a systematic

approach to training development, and has referenced NEI 06-13A, Revision 1. The staff finds this acceptable because it applies an NRC-endorsed approach.

## 13.3 Emergency Planning

This section addresses the plans, design features, facilities, functions, and equipment necessary for radiological emergency planning (EP) that must be considered in a COL application. This includes both the applicant's onsite emergency plan and State and local (offsite) emergency plans, which the NRC and the Federal Emergency Management Agency (FEMA) evaluate to determine whether the plans are adequate, and that there is reasonable assurance that they can be implemented. The plans shall be an expression of the overall concept of operation, and describe the essential elements of advance planning that have been considered and the provisions that have been made to cope with radiological emergency situations. This section of the safety evaluation is being provided under a separate letter and will be integrated with the rest of Chapter 13 at the final SER stage.

## 13.4 Operational Programs (Related to RG 1.206, Section C.III.1, Chapter 13, C.I.13.4, "Operational Program Implementation")

### 13.4.1 Introduction

In SECY-05-0197, "Review of Operational Programs in a Combined License Application and Generic Emergency Planning Inspections, Tests, Analyses, and Acceptance Criteria," dated October 28, 2005, the NRC staff detailed its plan for reviewing operational programs in a COL application. The Commission approved the NRC staff's plan in the related Staff Requirements Memorandum (SRM), dated February 22, 2006. Although numerous programs support the operation of a nuclear power plant, SECY-05-0197 focused on those programs that meet the following three criteria:

1. Required by regulation
2. Reviewed in a COL application
3. Inspected to verify program implementation as described in the FSAR

The programs that meet the above criteria are collectively referred to as "operational programs" and most are identified in SECY-05-0197.

### 13.4.2 Summary of Application

Section 13.4 of the VCSNS COL FSAR, Revision 2, incorporates by reference Section 13.4 of the AP1000 DCD, Revision 17.

In addition, in VCSNS COL FSAR Section 13.4 and in Part 10 of the VCSNS COL application, "Proposed License Conditions and ITAAC [inspections, tests, analyses, and acceptance criteria])," the applicant provided the following:

*AP1000 COL Information Item*

- STD COL 13.4-1

The applicant provided additional information in STD COL 13.4-1 to address COL Information Item 13.4-1 and COL Action Item 13.4-1, identified in Appendix F of NUREG-1793 and its supplements. This item states that COL applicants referencing the AP1000 certified design will address each operational program.

*License Conditions*

- Part 10, License Condition 3, "Operational Program Implementation"
- Part 10, License Condition 6, "Operational Program Readiness"

Both license conditions are related to STD COL 13.4-1. License Condition 3 addresses implementation milestones for those operational programs whose implementation is not addressed in the regulations. License Condition 6 includes the timing of information related to operational programs to support NRC inspection activities.

### 13.4.3 Regulatory Basis

The regulatory basis of the information incorporated by reference is addressed in NUREG-1793 and its supplements.

In addition, the regulatory basis for acceptance of the supplementary information presented in this application is identified in the individual chapters of this SER that address the evaluations of the specific operational programs, which are itemized in the next section, as clarified by the regulatory guidance in SECY-05-0197 and RG 1.206.

### 13.4.4 Technical Evaluation

The NRC staff reviewed Section 13.4 of the VCSNS COL FSAR and checked the referenced DCD to ensure that the combination of the DCD and the COL application represents the complete scope of information relating to this review topic.[1] The NRC staff's review confirmed that the information in the application and incorporated by reference addresses the required information relating to operational programs. The results of the NRC staff's evaluation of the information incorporated by reference in the VCSNS COL application are documented in NUREG-1793 and its supplements.

Section 1.2.3 of this SER provides a discussion of the strategy used by the NRC to perform one technical review for each standard issue outside the scope of the DC and use this review in evaluating subsequent COL applications. To ensure that the staff's findings on standard content that were documented in the SER for the reference COL application (VEGP

Units 3 and 4) were equally applicable to the VCSNS Units 2 and 3 COL application, the staff undertook the following reviews:

- The staff compared the VEGP COL FSAR, Revision 2 to the VCSNS COL FSAR. In performing this comparison, the staff considered changes made to the VCSNS COL FSAR (and other parts of the COL application, as applicable) resulting from RAIs.

- The staff confirmed that all responses to RAIs identified in the corresponding standard content evaluation were endorsed.

- The staff verified that the site-specific differences were not relevant.

The staff has completed its review and found the evaluation performed for the standard content to be directly applicable to the VCSNS COL application. This standard content material is identified in this SER by use of italicized, double-indented formatting. Section 1.2.3 of this SER provides an explanation of why the standard content material from the SER for the reference COL application (VEGP) includes evaluation material from the SER for the BLN Units 3 and 4 COL application.

The following portion of this technical evaluation section is reproduced from Section 13.4.4 of the VEGP SER:

> *Although the staff concluded that the evaluation performed for the standard content is directly applicable to the VEGP COL application, there were differences in the response provided by the VEGP applicant from that provided by the BLN applicant regarding the standard content material. These differences affect the two license conditions and the table listing the operational programs. These differences are evaluated by the staff below, following the standard content material.*
>
> *AP1000 COL Information Item*
>
> - *STD COL 13.4-1*
>
> *The applicant provided supplemental information by adding the following statement to Section 13.4 of the VEGP COL FSAR:*
>
> *Operational programs are specific programs that are required by regulations. Table 13.4-201 lists each operational program, the regulatory source for the program, the section of the FSAR in which the operational program is described, and the associated implementation milestone(s).*
>
> *Each operational program is evaluated by the staff in the applicable SER chapters.*

*License Conditions*

- *License Condition 3, "Operational Program Implementation"*
- *License Condition 6, "Operational Program Readiness"*

*These two proposed license conditions are evaluated by the NRC staff as part of its evaluation of each of the operational programs in the applicable SER chapters.*

*The following portion of this technical evaluation section provides the staff's general evaluation of the operational programs and associated license conditions and is reproduced from Section 13.4.4 of the BLN SER:*

*The NRC staff's review of the acceptability of the supplemental information added by STD COL 13.4-1 and the proposed license conditions is based on four considerations. The first consideration is the acceptability of the individual operational programs, including the implementation of the different phases of these operational programs. The second consideration is whether the applicant correctly identified those operational programs whose implementation requirements are not addressed in the regulations, and, therefore, need to be included in License Condition 3. The third consideration is whether the applicant correctly specified in License Condition 6 the timing of information related to operational programs to support NRC inspection activities. The fourth consideration is whether the list of operational programs in BLN COL FSAR Table 13.4-201 is complete.*

*In regard to the first consideration, the SER sections referenced in the above table address the NRC staff's regulatory evaluation of the individual operational programs. For each of these operational programs, the staff has either concluded that the applicant has satisfied the applicable regulatory guidance (including the implementation requirements when specified in the regulations), or the staff's review is still ongoing. For those operational program reviews that are ongoing, the staff's final conclusions will be provided in the SER sections referenced in the above table at a later date.*

*In regard to the second consideration, the NRC staff verified that those operational programs, whose implementation requirements are not specified in the regulations, are captured in License Condition 3.*

*In regard to the third consideration, the NRC staff compared License Condition 6 to the recommended license condition in SECY-05-0197 related to the timing of information to support NRC inspection activities of operational programs. The staff finds that the applicant used language similar to the recommended license condition specified in SECY-05-0197 to develop License Condition 6. It should be noted that License Condition 6 addresses additional scheduler requirements (Sections b. through d.) that are not related to the operational programs*

*evaluated in this section of the SER, and, therefore, are not evaluated in this SER section.*

*In regard to the fourth consideration, the NRC staff compared the operational programs provided by the applicant in BLN COL FSAR Table 13.4-201 (included in the above table) to the operational programs specified in SECY-05-0197. The staff finds that the applicant has included all the operational programs specified in SECY-05-0197, including the two operational programs (Motor-Operated Valve Testing Program and the Safeguards Contingency Program) added by the NRC to the list of operational programs provided by the NEI in its letter dated August 31, 2005.*

*There are differences between BLN COL FSAR Table 13.4-201 and the table of operational programs in SECY-05-0197 with respect to implementation milestone information. The first difference is the SECY paper states that there are no required implementation milestones in the regulations for the Maintenance Rule Program and the Quality Assurance Program (Operation), while BLN COL FSAR Table 13.4-201 references regulations that require implementation milestones for these two programs. The staff has reviewed the regulation references provided by the applicant and concludes that they do provide appropriate requirements for implementation milestones. Further support for this conclusion is the regulatory guidance in Section C.I.13.4 of RG 1.206. The example table located in this section of the RG references the same implementation regulatory guidance for the Maintenance Rule Program and the Quality Assurance Program (Operation) as does BLN COL FSAR Table 13.4-201.*

*The second difference is that the SECY paper states that 10 CFR Part 50, Appendix J, specifies implementation requirements for the Containment Leakage Rate Testing Program, while BLN COL FSAR Table 13.4-201 states that the implementation milestones for this program will be controlled by a license condition. The staff has reviewed the implementation milestone proposed in License Condition 3 for the Containment Leakage Rate Testing Program, and finds that it is more stringent than the regulatory guidance in Appendix J. Therefore, the staff finds this difference to be acceptable.*

*The applicant added an operational program to BLN COL FSAR Table 13.4-201, the Initial Test Program, which is not in the list of operational programs specified in SECY-05-0197. The option of adding operational programs to this list is specifically allowed by SECY-05-0197. Further support for the acceptability of adding the Initial Test Program is that the example table located in Section C.I.13.4 of RG 1.206 also lists this operational program.*

*Therefore, the NRC staff concludes that the additional information (STD COL 13.4-1) provided by the applicant in BLN COL FSAR Section 13.4, in conjunction with the conditions specified in BLN COL FSAR, Part 10, License Conditions 3 and 6, complies with the applicable regulatory guidance provided in SECY-05-0197.*

*Evaluation of Site-specific Response to Standard Content*

*The staff notes that the VEGP applicant separated the fitness-for-duty (FFD) program from the overall security program and added a new operational program, Cyber Security, to the list of operational programs in FSAR Table 13.4-201. The implementation requirements for these additional operational programs comply with the considerations identified above in the standard content material, and are, therefore, acceptable. In addition, the VEGP applicant also made minor changes to operational program implementation details in License Condition 3 and also modified Sections a. through d. associated with License Condition 6. The changes to these two license conditions are evaluated by the staff in the applicable SER chapters and do not affect the evaluation of operational programs covered in this section of the SER. Therefore, the conclusions reached by the NRC staff related to STD COL 13.4-1 are directly applicable to the VEGP COL application.*

*The BLN SER text refers to an SER table listing operational programs. This table was not reproduced for the VEGP SER since it duplicates the information in VEGP COL FSAR Table 13.4-201.*

### 13.4.5 Post Combined License Activities

The license conditions for each of the operational programs are discussed in the applicable SER chapters. Therefore, there are no post-COL activities related to this section.

### 13.4.6 Conclusion

The NRC staff reviewed the application and checked the referenced DCD. The NRC staff's review confirmed that the applicant addressed the required information relating to operational programs, and there is no outstanding information expected to be addressed in the VCSNS COL FSAR related to this section. The results of the NRC staff's technical evaluation of the information incorporated by reference in the VCSNS COL application are documented in NUREG-1793 and its supplements.

The staff concludes that the relevant information presented in the VCSNS COL FSAR is acceptable based on the regulatory guidance in SECY-05-0197, in conjunction with the applicable regulations specified in the individual sections of this SER that evaluated each of the operational programs discussed above. The staff based its conclusion on the following:

- STD COL 13.4-1, as related to operational programs, is acceptable because each of the operational programs in VCSNS COL FSAR Table 13.4-201 has been found acceptable by the NRC staff in other sections of this SER, as noted in Section 13.4.4 above. In addition, the guidance in SECY-05-0197 and RG 1.206 was used to verify that the applicant's list of operational programs is complete.

## 13.5 Plant Procedures

### 13.5.1 Introduction

Descriptions of the administrative and operating procedures that the applicant uses to ensure routine operating, off-normal, and emergency activities are conducted in a safe manner are provided. The applicant, in its plant procedures, provided a brief description of the nature and content of the procedures and a schedule for the preparation of appropriate written administrative and operating procedures. The applicant delineated in the description of the procedures the functional position for procedural revision and approval prior to implementation. Inspection of procedures will occur as part of the construction inspection program.

### 13.5.2 Summary of Application

Section 13.5 of the VCSNS COL FSAR, Revision 2, incorporates by reference Section 13.5 of the AP1000 DCD, Revision 17.

In addition, in VCSNS COL FSAR Section 13.5, the applicant provided the following:

*AP1000 COL Information Item*

- STD COL 13.5-1

The applicant provided additional information in STD COL 13.5-1 to resolve COL Information Item 13.5-1 (COL Action Item 13.5-1), which addresses plant procedures.

*Supplemental Information*

- VCS SUP 13.5-1 and VCS SUP 13.5-2

The applicant provided plant-specific supplemental information in VCS SUP 13.5-1 and VCS SUP 13.5-2 to resolve COL Information Item 13.5-1 (COL Action Item 13.5-1), which addresses plant procedures.

### 13.5.3 Regulatory Basis

The regulatory basis of the information incorporated by reference is addressed in NUREG-1793 and its supplements.

In addition, the acceptance criteria associated with the relevant requirements of the Commission regulations for plant procedures are given in Sections 13.5.1.1 and 13.5.2.1 of NUREG-0800.

The applicable regulations and regulatory guidance are as follows:

- 10 CFR 50.34(a), “Preliminary safety analysis report”
- 10 CFR 50.34(b), “Final safety analysis report”
- RG 1.33

### 13.5.4 Technical Evaluation

The NRC staff reviewed Section 13.5 of the VCSNS COL FSAR and checked the referenced DCD to ensure that the combination of the DCD and the COL application represents the complete scope of information relating to this review topic.[1] The NRC staff's review confirmed that the information in the application and incorporated by reference addresses the required information relating to plant procedures. The results of the NRC staff's evaluation of the information incorporated by reference in the VCSNS COL application are documented in NUREG-1793 and its supplements.

Section 1.2.3 of this SER provides a discussion of the strategy used by the NRC to perform one technical review for each standard issue outside the scope of the DC and use this review in evaluating subsequent COL applications. To ensure that the staff's findings on standard content that were documented in the SER for the reference COL application (VEGP Units 3 and 4) were equally applicable to the VCSNS Units 2 and 3 COL application, the staff undertook the following reviews:

- The staff compared the VEGP COL FSAR, Revision 2 to the VCSNS COL FSAR. In performing this comparison, the staff considered changes made to the VCSNS COL FSAR (and other parts of the COL application, as applicable) resulting from RAIs.

- The staff confirmed that all responses to RAIs identified in the corresponding standard content evaluation were endorsed.

- The staff verified that the site-specific differences were not relevant.

The staff has completed its review and found the evaluation performed for the standard content to be directly applicable to the VEGPCSNS COL application. This standard content material is identified in this SER by use of italicized, double-indented formatting. Section 1.2.3 of this SER provides an explanation of why the standard content material from the SER for the reference COL application (VEGP) includes evaluation material from the SER for the BLN Units 3 and 4 COL application.

The following portion of this technical evaluation section is reproduced from Section 13.5.4 of the VEGP SER:

*AP1000 COL Information Item*

- *STD COL 13.5-1, addressing plant procedures*

*The applicant provided the following additional information to resolve COL Information Item 13.5-1, which addresses the plant procedures of the COL applicant. COL Information Item 13.5-1 states:*

*Combined License applicants referencing the AP1000 certified design will address plant procedures including the following:*

- *Normal operation*
- *Abnormal operation*
- *Emergency operation*
- *Refueling and outage planning*
- *Alarm response*
- *Maintenance, inspection, test and surveillance*
- *Administrative*
- *Operation of post-72 hour equipment*

*The commitment was also captured as COL Action Item 13.5-1 in Appendix F of the staff's FSER for the AP1000 DCD (NUREG-1793).*

*The applicant provided additional text in BLN COL FSAR Section 13.5 to describe the administrative, operating and maintenance procedures that the operating organizational staff uses to conduct routine operating, abnormal, and emergency activities in a safe manner.*

*In BLN COL FSAR Section 13.5, the applicant described the different classifications of procedures that the operators will use, including normal, abnormal, emergency, refueling and outage, and alarm response procedures. The staff finds this information acceptable because it meets the criteria in NUREG-0800, Chapter 13.5.2.1.*

*In BLN COL FSAR Section 13.5, the applicant stated that the format and content of procedures are controlled by the applicable AP1000 writer's guideline. The DCD, Section 13.5.1, describes a referenced document, APP-GW-GLR-040, "Plant Operations Maintenance and Surveillance Procedures," dated August 23, 2007, which includes the AP1000 writer's guidelines. The staff finds this acceptable because the applicant-provided procedure format and content are consistent with the guidance in NUREG-0800, Section 13.5.2.1.*

*In BLN COL FSAR Section 13.5.1, the applicant describes the nature and content of administrative procedures for both Category (A) - Controls, and Category (B) - Specific Procedures. The staff finds this acceptable because the listed procedures are consistent with the guidance in NUREG-0800, Section 13.5.1.1.*

*In BLN COL FSAR Section 13.5.2, the applicant stated that EP procedures are discussed in the Emergency Plan and that security procedures are discussed in the Security Plan. The evaluation of EP procedures may be found in Section 13.3 of this SER. The evaluation of security procedures is found in Section 13.6 of this SER.*

*In BLN COL FSAR Section 13.5.2, the applicant stated the Quality Assurance Program description (QAPD) provides a description of procedural requirements for maintenance, instrument calibration and testing, inspection, and material*

*control. The evaluation of QAPD procedures is found in Section 17.5 of this SER.*

*In BLN COL FSAR, Section 13.5.2.1, the applicant stated that information related to EOPs is addressed in the DCD. The DCD, Section 13.5.1, describes the program for developing and implementing EOPs and the required content of EOPs procedures in the referenced document, APP-GW-GLR-040. In addition, this information clarifies the procedure development program (PDP) as described in the procedures generation package (PGP) for EOPs, provides a description of the EOP* [emergency operating plan] *verification and validation (V&V) program, and describes the program for training operators on EOPs, including an explanation of how the recommendations of TMI Action Plan, Item I.C.1, will be met. The staff finds the program for developing and implementing EOPs acceptable because it meets the criteria in NUREG-0800, Section 13.5.2.1.*

*Evaluation of Plant Procedure Issues Not Address in the Standard Content Evaluation*

*In VEGP COL FSAR Table 1.9-202, "Conformance with SRP Acceptance Criteria," the applicant identified two exceptions to the criteria of NUREG-0800, Section 13.5, which recommends providing a schedule for procedure development in the FSAR, and including a description of procedures to be used by operators in the FSAR. The staff notes that the BLN COL FSAR Table 1.9-202 includes these same two exceptions to the criteria of Section 13.5 of NUREG-0800. The guidance of NUREG-0800, Section 13.5.2.1, states that while the submittal should describe the different classifications of procedures that operators will use, it is not necessary that each applicant's procedures conform precisely. In addition, the procedures, regardless of title or classification, are to be available to accomplish the functions identified in RG 1.33. NUREG-0800 makes allowance for "general areas." The staff finds the two exceptions to the criteria of NUREG-0800, Section 13.5 to be acceptable because the applicant's procedure classification follows the guidance in NUREG-0800, Section 13.5.*

*In RAI* [request for additional information] *13.6-36, the staff requested the VEGP applicant address the requirements of 10 CFR 73.58, "Safety/security requirements for nuclear power plants." In its response dated May 14, 2010, the applicant stated that management controls and processes used to establish and maintain an effective interface between nuclear safety and physical security are addressed by administrative controls. The VEGP applicant committed to revise FSAR Section 13.5.1 to include the safety/security interface implementation process in the list of procedural instructions provided in plant administrative procedures. The NRC staff's review of this safety/security procedural issue, which includes tracking the incorporation of the relevant material into the VEGP COL application, is addressed in Section 13.6.4.1.17 of this SER.*

*Supplemental Information*

- VCS SUP 13.5-1 and VCS SUP 13.5-2

In VCSNS COL FSAR Section 13.5.1, the applicant provides plant-specific supplemental information describing the nature and content of administrative procedures for specific procedures. The staff finds this acceptable because the listed procedures are consistent with the guidance in NUREG-0800, Sections 13.5.1.1 and 13.5.2.1.

### 13.5.5 Post Combined License Activities

There are no post-COL activities related to this section.

### 13.5.6 Conclusion

The NRC staff reviewed the application and checked the referenced DCD. The NRC staff's review confirmed that the applicant addressed the required information relating to plant procedures, and there is no outstanding information expected to be addressed in the VCSNS COL FSAR related to this section. The results of the NRC staff's technical evaluation of the information incorporated by reference in the VCSNS COL application are documented in NUREG-1793 and its supplements.

In addition, the staff concludes that the relevant information presented in the VCSNS COL FSAR is acceptable and meets the recommendations of NUREG-0800, Sections 13.5.1.1 and 13.5.2.1. The staff based its conclusion on the following:

- STD COL 13.5-1, as related to plant procedures, is acceptable because it describes the procedures used by the applicant's operating organizational staff to conduct routine administrative, operating, abnormal, and emergency activities in a safe manner, in accordance with the regulatory guidance in NUREG-0800, Sections 13.5.1.1 and 13.5.2.1.

- VCS SUP 13.5-1 and VCS SUP 13.5-2, as related to plant-specific plant procedures, is acceptable because they describe procedures used by the applicant's operating organizational staff to conduct routine administrative, operating, abnormal, and emergency activities in a safe manner, in accordance with the regulatory guidance in NUREG-0800, Sections 13.5.1.1 and 13.5.2.1.

- In VCSNS COL FSAR Table 1.9-202, the applicant identified two exceptions to the criteria of NUREG-0800, Section 13.5, related to providing FSAR descriptions of, and a development schedule for, procedures to be used by operators. The guidance of NUREG-0800, Section 13.5.2.1, makes allowances for "general areas," stating that while the FSAR submittal should describe the different classifications of procedures used by operators, it is not expected that each applicant's procedures conform precisely. The staff finds the two exceptions to be acceptable because the applicant's procedure classification follows the guidance in NUREG-0800, Section 13.5.

## 13.6 Physical Security

### 13.6.1 Introduction

The COL application for the VCSNS Units 2 and 3 describes the COL applicant's physical protection program, which is intended to meet NRC regulations for protection against the design basis threat (DBT) of radiological sabotage as stated in 10 CFR 73.1 and provide a high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.

The physical protection program includes the design of a physical protection system that ensures the capabilities to detect, assess, interdict, and neutralize threats of radiological sabotage are maintained at all times. The applicant incorporates by reference the standard AP1000 design that includes design of physical protection systems within the design of the vital island and vital structures, as described in the Westinghouse Electric Company (Westinghouse) design certification document for the AP1000 standard design Tier 1 and Tier 2 information, including Technical Report (TR)-49, "AP1000 Enhancement Report, TR-94, "AP1000 Safeguards Assessment Report," and TR-96, "Interim Compensatory Measures Report." Part 8 of the COL application consists of the VCSNS Units 2 and 3 Physical Security Plan (PSP), Training and Qualification Plan (T&QP), and Safeguards Contingency Plan (SCP). Section 13.6 of the VCSNS COL FSAR describes the physical protection program and the physical protection system that are not addressed within the scope of the standard AP1000 design for meeting NRC performance and prescriptive requirements for physical protection stated in 10 CFR Part 73, "Physical Protection of Plants and Material." Those persons with the correct access authorization and need-to-know may view the safeguards information version of the VCSNS COL application Section 13.6 SER, which is located in the NRC's Secure Local Area Network, document number ES100015156.

### 13.6.2 Summary of Application

Section 13.6 of the VCSNS COL FSAR, Revision 2, incorporates by reference Section 13.6 of the AP1000 DCD, Revision 17.

Part 8 – Safeguards/Security Plans

In a letter dated March 27, 2008, South Carolina Electric & Gas (SCE&G) submitted a PSP to the NRC as part of the COL application for proposed VCSNS Units 2 and 3. In a letter dated April 2, 2009, SCE&G submitted Revision 1 to the PSP. In a letter dated August 14, 2010, SCE&G submitted Revision 2 to its PSP.

In addition, in VCSNS COL FSAR Section 13.6, the applicant provided the following:

*AP1000 COL Information Items*

- STD COL 13.6-1

The applicant provided additional information in STD COL 13.6-1 to address COL Information Item 13.6-1, which provides information related to the security plan. The security plan consists of three parts, the PSP, T&QP, and SCP.

- STD COL 13.6-5

The applicant provided additional information in STD COL 13.6-5 to address COL Information Item 13.6-5, which provides information related to the cyber security program. This COL item is evaluated in Section 13.8 of this SER.

*License Conditions*

- Part 10, License Condition 3, Items C.5, D.3, and G.9

The applicant proposed a license condition in Part 10 of the VCSNS COL application, which provides the milestones for implementing applicable portions of the Security Program.

- Part 10, License Condition 5

The applicant proposed a license condition in Part 10 of the VCSNS COL application, which proposed the maintenance of the PSP, T&QP, and the SCP when nuclear fuel is onsite, and continuing until all nuclear fuel is permanently removed from the site.

- Part 10, License Condition 6

The applicant proposed a license condition to provide a schedule to support the NRC's inspection of operational programs including the PSP, T&QP, and the SCP.

### 13.6.3 Regulatory Basis

The regulatory basis of the information incorporated by reference is addressed in NUREG-1793, and its supplements.

The applicable regulatory requirements for physical protection are as follows:

- The provisions of 10 CFR 52.79(a)(35)(i) and (ii) require that information submitted for a (COL) describe how the applicant will meet the requirements of 10 CFR Part 73, "Physical Protection of Plants and Material"; and provide a description of the implementation of the PSP. The provisions of 10 CFR 52.79(a)(36)(i) through (v) require that the application include an SCP in accordance with the criteria set forth in Appendix C to 10 CFR Part 73, and a T&QP in accordance with Appendix B of

10 CFR Part 73, that the applicant provide a description of the implementation of the SCP and the T&QP and that the applicant protect the PSP, SCP and T&QP in accordance with the requirements of 10 CFR 73.21, "Protection of Safeguards Information: Performance Requirements."

- The provisions of 10 CFR Part 73 include performance-based and prescriptive regulatory requirements that, when adequately met and implemented, provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety. A COL applicant must describe how it will meet the regulatory requirements of 10 CFR Part 73 that are applicable to nuclear power plants.

A COL applicant is required to identify and describe design features, analytical techniques, and technical bases for its design and how it will meet provisions of physical protection system requirements in the NRC regulations, using applicable RGs and NUREG-0800. However, the NRC RGs and NUREG-0800 are not regulatory requirements and are not a substitute for compliance with established regulations. Where alternative methods are chosen or differences exist, the COL applicant is required to describe how the proposed alternatives to guidance or acceptance criteria provide acceptable methods of compliance with the NRC regulations.

NUREG-0800 Section 13.6.1, Revision 1, June 15, 2010 was used by the NRC staff to complete the physical security COL review.

Regulatory guidance documents, TRs, and accepted industry codes and standards that an applicant may apply to meet regulatory requirements include, but are not limited to the following:

- RG 5.7, "Entry/Exit Control for Protected Areas, Vital Areas, and Material Access Areas," Revision 1
- RG 5.12, "General Use of Locks in the Protection and Control of Facilities and Special Nuclear Materials"
- RG 5.44, "Perimeter Intrusion Alarm Systems," Revision 3
- RG 5.62, "Reporting of Safeguards Events," Revision 1
- RG 5.65, "Vital Area Access Controls, Protection of Physical Protection System Equipment and Key and Lock Controls"
- RG 5.66, "Access Authorization Program for Nuclear Power Plants"
- RG 5.68, "Protection Against Malevolent Use of Vehicles at Nuclear Power Plants"
- RG 5.74, "Managing the Safety/Security Interface"
- RG 5.75, "Training and Qualification of Security Personnel at Nuclear Power Reactor Facilities"

- NRC letter dated April 9, 2009, NRC Staff Review of NEI 03-12, "Template for Security Plan, Training and Qualification, Safeguards Contingency Plan, [and Independent Spent Fuel Storage Installation Security Program]" (Revision 6)

- SECY-05-0197, "Review of Operational Programs in a Combined License Application and Generic Emergency Planning Inspections, Tests, Analyses, and Acceptance Criteria," October 28, 2005

The following documents include security-related or safeguards information and are not publicly available:

- RG 5.69, "Guidance for the Application of Radiological Sabotage Design Basis Threat in the Design, Development, and Implementation of a Physical Security Protection Program that Meets 10 CFR 73.55 Requirements"

- RG 5.76, "Physical Protection Programs at Nuclear Power Reactors"

- NEI 03-12, Revision 6, "Template for the Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, and Independent Spent Fuel Installation Security Program"

- NUREG/CR-6190, "Update of NUREG/CR-6190 Material to Reflect Postulated Threat Requirements"

### 13.6.4 Technical Evaluation

The NRC staff reviewed Section 13.6 of the VCSNS COL FSAR and checked the referenced DCD to ensure that the combination of the DCD and the COL application represents the complete scope of information relating to this review topic.[1] The NRC staff's review confirmed that the information in the application and incorporated by reference addresses the required information relating to physical security. The results of the NRC staff's evaluation of the information incorporated by reference in the VCSNS COL application are documented in NUREG-1793 and its supplements.

Section 1.2.3 of this SER provides a discussion of the strategy used by the NRC to perform one technical review for each standard issue outside the scope of the DC and use this review in evaluating subsequent COL applications. To ensure that the staff's findings on standard content that were documented in the SER for the reference COL application (VEGP Units 3 and 4) were equally applicable to the VCSNS Units 2 and 3 COL application, the staff undertook the following reviews:

- The staff compared the VEGP COL FSAR, Revision 2 to the VCSNS COL FSAR. In performing this comparison, the staff considered changes made to the VCSNS COL FSAR (and other parts of the COL application, as applicable) resulting from RAIs.

- The staff compared the VEGP PSP, T&QP, and SCP to the corresponding VCSNS programs. The staff has determined that these plans are sufficiently similar to warrant standard content treatment.

- The staff confirmed that all responses to RAIs identified in the corresponding standard content evaluation were endorsed.

- The staff verified that the site-specific differences were not relevant.

The staff has completed its review and found the evaluation performed for the standard content to be directly applicable to the VCSNS COL application, with the exception discussed in the following paragraph. This standard content material is identified in this SER by use of italicized, double-indented formatting. One clarification to the standard content material presented below is that the NRC staff's detailed evaluation of the physical protection program, which is site-specific, is provided in the safeguards information version of the VCSNS COL application Section 13.6 SER, which is located in the NRC's Secure Local Area Network, document number ES1000015156.

There were site-specific RAIs issued to the VCSNS applicant that resulted in site-specific evaluations for several of the Security Plan review areas. There were also site-specific RAIs issued to the VEGP applicant that were not applicable to the VCSNS application. In addition, there are several Security Plan review areas with site-specific characteristics requiring a specific review by the staff. For these cases, the staff provides the VCSNS evaluation in the same location as provided in the VEGP SER, but without the use of italicized, double-indented formatting.

The following portion of this technical evaluation section is reproduced from Section 13.6.4 of the VEGP SER:

*AP1000 COL Information Item*

- *STD COL 13.6-1*

*The NRC staff reviewed STD COL 13.6-1 related to COL Information Item 13.6-1, which identified the need for a COL applicant to address the security plan. STD COL 13.6-1 supplemented Section 13.6 of the VEGP COL FSAR by stating the following text is to be added after Section 13.6 of the VEGP ESP SSAR:*

> *The Security Plan consists of the Physical Security Plan, the Training and Qualification Plan, and the Safeguards Contingency Plan. The Security Plan is submitted to the Nuclear Regulatory Commission as a separate licensing document in order to fulfill the requirements of 10 CFR 52.79(a)(35) and 52.79(a)(36). The Security Plan meets the requirements contained in 10 CFR Part 73 and will be maintained in accordance with the requirements of 10 CFR 52.98. The Plan is categorized as*

*Security Safeguards Information and is withheld from public disclosure pursuant to 10 CFR 73.21.*

*Section 13.6 of the VEGP COL FSAR also refers to FSAR Table 13.4-201, "Operational Programs Required by NRC Regulations," as providing the milestones for implementing the security program and cyber security program.*

*The NRC staff's evaluation of the PSP is documented in Section 13.6.4.1 of this SER. The NRC staff's evaluation of the T&QP is documented in Section 13.6.4.2 of this SER. The NRC staff's evaluation of the SCP is documented in Section 13.6.4.3 of this SER. The NRC staff's evaluation of the safety/security interface is documented in Section 13.6.4.1.17 of this SER. Section 13.6.5 of this SER includes the post-combined license activities. Section 13.6.6 of this SER includes the NRC staff's overall conclusions regarding each of the plan submissions.*

*The NRC staff's evaluation of the physical protection program is provided in detail in the safeguards information version of the VEGP COL application Section 13.6 SER, which is located in the NRC's Secure Local Area Network, document number ES1000015157. Due to security restraints, the NRC staff's evaluation of the physical protection program presented in this publicly-available SER does not include the same level of detail as the safeguards information version. Those persons with the correct access authorization and need-to-know may view the safeguards information version of the VEGP COL application Section 13.6 SER.*

*<u>License Conditions</u>*

- *Part 10, License Condition 3, Items C.5, D.3, and G.9*

*The applicant provided a license condition in Part 10 of the VEGP COL application, which provides the milestones for implementing applicable portions of the Security Program. Specifically, the applicant proposed the following:*

> *C. Receipt of Materials – The licensee shall implement each operational program identified below prior to initial receipt of byproduct, source, or special nuclear materials onsite (excluding Exempt Quantities as described in 10 CFR 30.18).*
>
> *C.5 – Security Program (applicable portions)*
>
> *D. Fuel Receipt – The licensee shall implement each operational program identified below prior to initial receipt of fuel onsite.*
>
> *D.3 – Security Program (applicable portions)*

> *G. Fuel Loading – The licensee shall implement each operational program identified below prior to initial fuel load.*
> *G.9 – Physical Security*

- *Part 10, License Condition 5*

*The applicant provided a license condition in Part 10 of the VEGP COL application, which proposed the maintenance of the PSP, T&QP, and the SCP when nuclear fuel is onsite, and continuing until all nuclear fuel is permanently removed from the site. Specifically, the applicant proposed the following:*

> *The licensee shall maintain in effect the provisions of the physical security plan, security personnel training and qualification plan, and safeguards contingency plan, and all amendments made pursuant to the authority of 10 CFR 50.90, 50.54(p), 52.97, and Section VIII of Appendix D to Part 52 when nuclear fuel is onsite, and continuing until all nuclear fuel is permanently removed from the site.*

*In a letter dated October 22, 2010, the applicant proposed to revise the* [security plan] *milestone included in VEGP COL FSAR Table 13.4-201 to implement the* [security plan] *prior to receipt of fuel onsite (protected area.) The NRC staff finds the implementation milestone for the security ~~program~~*[plan] *(~~security~~ prior to receipt of fuel onsite (protected area)) appropriate and in accordance with the requirement in 10 CFR 73.55. Therefore the staff finds that the proposed License Condition 3, Items C.5, D.3, and G.9 and License Condition 5 are not necessary. The incorporation of proposed changes to the VEGP COL FSAR are tracked as* ***Confirmatory Item 13.6-1.***

- *Part 10, License Condition 6*

*The applicant proposed a license condition to provide a schedule to support the NRC's inspection of operational programs including the PSP, T&QP, and the SCP. Specifically, the applicant proposed the following:*

> *The licensee shall submit to the appropriate Director of the NRC, a schedule, no later than 12 months after issuance of the COL, that supports planning for and conduct of NRC inspections of operational programs listed in the operational program FSAR Table 13.4-201. The schedule shall be updated every 6 months until 12 months before scheduled fuel loading, and every month thereafter until either the operational programs in the FSAR table have been fully implemented or the plant has been placed in commercial service, whichever comes first.*

*The staff reviewed the above proposed license condition against the recommendations in SECY-05-0197 as endorsed by the related SRM dated*

*February 22, 2006. The staff concludes these proposed license conditions conform to the guidance in SECY-05-0197 and is, therefore, acceptable.*

*13.6.4.1 Physical Security Plan*

*The applicant submitted Part 8 of the COL application for the VEGP PSP, T&QP and SCP, to meet the requirements of 10 CFR 52.79(a)(35) and (36). Part 2, FSAR, Chapter 13, Section 13.6 references the VEGP PSP, T&QP, and SCP in describing the licensing basis for establishing a physical protection program, design of a physical protection system, and security organization, which will have, as its objective, to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety. The VEGP submitted PSP makes references to 10 CFR 50.34(c)(2) and (d)(2). The correct references should be 10 CFR 52.79(a)(35) and (36). It is noted that this is a template error, and both references require that the same criteria be met.*

*Security plans must describe how the applicant will implement Commission requirements and those site-specific conditions that affect implementation as required by 10 CFR 73.55(c)(1)(i).*

*The requirements are provided in 10 CFR 73.55(c), and (d) to establish, maintain, and implement a PSP to meet the requirements of 10 CFR 73.55, and 10 CFR Part 73, Appendices B and C. The applicant must show establishment and maintenance of a security organization, the use of security equipment and technology, the training and qualification of security personnel, the implementation of predetermined response plans and strategies, and the protection of digital computer and communication systems and networks. The applicant must have a management system for development, implementation, revision, and oversight of security implementing procedures. The approval process for implementing security procedures will be documented.*

*The NRC staff has reviewed the applicant's description in PSP Section 1 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the PSP meets the requirements of 10 CFR 73.55(c) and (d), and is, therefore, acceptable.*

13.6.4.1.1 Introduction and Physical Facility Layout

The provisions of 10 CFR 52.79(a)(35):

(i) A PSP, describing how the applicant will meet the requirements of 10 CFR Part 73 (and 10 CFR Part 11, if applicable, including the identification and description of jobs as required by 10 CFR 11.11(a) of this chapter, at the proposed facility). The plan must list

tests, inspections, audits, and other means to be used to demonstrate compliance with the requirements of 10 CFR Parts 11 and 73, if applicable;

(ii) A description of the implementation of the PSP;

The provisions of 10 CFR 52.79(a)(36) require:

(i) An SCP in accordance with the criteria set forth in Appendix C to 10 CFR Part 73. The safeguards contingency plan shall include plans for dealing with threats, thefts, and radiological sabotage, as defined in 10 CFR Part 73 of this chapter, relating to the special nuclear material and nuclear facilities licensed under this chapter and in the applicant's possession and control. Each application for this type of license shall include the information in the applicant's SCP. (Implementing procedures required for this plan need not be submitted for approval);

(ii) A T&QP in accordance with the criteria set forth in Appendix B to 10 CFR Part 73;

(iii) A cyber security plan (CSP) in accordance with the criteria set forth in 10 CFR 73.54 of this chapter;

(iv) A description of the implementation of the SCP, T&QP, and CSP; and

(v) Each applicant who prepares a PSP, an SCP, a T&QP, or a CSP, shall protect the plans and other related Safeguards Information against unauthorized disclosure in accordance with the requirements of 10 CFR 73.21 of this chapter.

The provisions of 10 CFR 52.79(a)(44) require a description of the FFD program required by 10 CFR Part 26 and its implementation.

Requirements are established in 10 CFR 73.55(c)(2) to ensure protection of safeguards information (SGI) against unauthorized disclosure in accordance with 10 CFR 73.21. The applicant’s submittal acknowledges that the PSP, the TQ&P and the SCP discuss specific features of the physical security system or response procedures and are SGI.

Section 1 of the PSP describes the applicant’s commitment to satisfying 10 CFR 50.34(c), 10 CFR 50.34(d) and 10 CFR Part 73 by submitting a PSP, and to controlling the PSP and appendices as Safeguards Information according to 10 CFR 73.21.

The provisions of 10 CFR Part 73, Appendix C, Section II.B.3.b, requires a description of the physical layout of the site.

Section 1.1 of the PSP provides descriptions of location, site layout, and facility configuration. The PSP describes the physical structures and their locations on the site, description of the protected area, and a description of the site in relation to nearby town, roads, and other environmental features important to the coordination of response operations. The plant layout includes identification of main and alternate entry routes for law enforcement assistance forces and the location of control points for marshalling and coordinating response activities.

In addition, Section 1.2 of the VCSNS COL application provides general plant descriptions that include details of the 10 to 50 mile radius of the geographical area of the VCSNS Units 2 and 3 site, a site area map, and general plant and site descriptions. VCSNS COL FSAR, Chapter 1, references the AP1000 DCD for the principal design and operating characteristics for the design and construction of the VCSNS Units 2 and 3. Part 1, General Information, of the VCSNS COL application describes the name of the applicant and principal business locations.

The NRC staff has reviewed the facility physical layout provided in Section 1.1 of the PSP and as supplemented by VCSNS COL FSAR. The NRC staff determined that the applicant included site-specific conditions that affect the applicant's capability to satisfy the requirements of a comprehensive PSP. The applicant has adequately described the physical structures and their locations onsite and the site in relation to nearby towns, roads, and other environmental features important to the effective coordination of response operations. The applicant described the main and alternate entry routes for law-enforcement assistance forces and the location of control points for marshaling and coordinating response activities in the site-specific law enforcement response plan. The NRC staff concludes that the applicant's security plans have met the requirements for content of a PSP as stated above. Therefore, the NRC staff finds the "Facility Layout" described in the PSP and the VCSNS COL FSAR is adequate.

The following portion of this technical evaluation section is reproduced from Section 13.6.4.1 of the VEGP SER:

> *13.6.4.1.2 Performance Objectives*
>
> *The provisions of 10 CFR 73.55(b)(1) requires, in part, that the applicant shall establish and maintain a physical protection program with an objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety. The provisions of 10 CFR 73.55(b)(2) establish, in part, the requirement to protect a nuclear power reactor against the DBT of radiological sabotage as described in 10 CFR 73.1*,[. The provisions of ] *10 CFR 73.55(b)(3)(i), and 10 CFR 73.55(b)(3)(ii) require the applicant to establish a physical protection program designed to ensure the capabilities to detect, assess, interdict, and neutralize threats up to and including the DBT of radiological sabotage as stated in 10 CFR 73.1, are maintained at all times, provide defense-in-depth, supporting processes, and implementing procedures, which ensure the effectiveness of the physical protection program.*
>
> *Section 2 of the PSP outlines the requirements for the establishment and maintenance of an onsite physical protection system, security organization, and integrated response capability. As part of the objective, the security program design shall incorporate supporting processes such that no single event can disable the security response capability because of defense-in-depth principles including diversity and redundancy. The physical protection systems and programs described herein are designed to protect against the DBT of radiological sabotage in accordance with the requirements of 10 CFR 73.55(a)*

*through (r) or equivalent measures that meet the same high assurance objectives provided by paragraph (a) through (r). VEGP Units 3 and 4 uses the corrective action program to track, trend, correct and prevent recurrence of failures and deficiencies in the physical protection program.*

*The NRC staff has reviewed the applicant's description in PSP Section 2 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the PSP meets the requirements of 10 CFR 73.55(b), and is, therefore, acceptable.*

*13.6.4.1.3 Performance Evaluation Program*

*Requirements are established in 10 CFR 73.55(b)(4) through (b)(11) for the applicant to analyze and identify site-specific conditions, establish programs, plans, and procedures that address performance evaluations, access authorization, cyber security, insider mitigation, fitness for duty (FFD), corrective actions, and operating procedures. 10 CFR 73.55(b)(6) prescribes specific requirements to establish, maintain, and implement a performance evaluation program in accordance with 10 CFR Part 73, Appendix B, Section VI for implementation of the plant protective strategy.*

*Section 3.0 of the PSP describes that drills and exercises, as discussed in the T&QP, will be used to assess the effectiveness of the contingency response plan and the effectiveness of the applicant's response strategy. Other assessment methods include formal and informal exercises or drills, self-assessments, internal and external audits and evaluations.*

*The performance evaluation processes and criteria that assess the effectiveness of the security program, including adequate protection against radiological sabotage, will be established in facility procedures and the deficiencies identified are managed through the corrective action program.*

*Section 3.0 of the PSP references Section 4.0 of the T&QP, which provides additional details related to the performance evaluation of security personnel in accordance with 10 CFR Part 73, Appendix B, Section VI. Section 4.0 of the T&QP includes the requirements to conduct security force tactical ~~dills~~* [drills] *and force-on-force exercises to evaluate security systems effectiveness and response performances of security personnel. In addition, Section 17 of the PSP describes additional detail regarding the applicant's processes for reviews, evaluations and audits that will complement the performance evaluation program.*

*The NRC staff has reviewed the applicant's description in PSP Section 3, for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in*

*NUREG-0800, Section 13.6.1, the staff finds that the description provided in the PSP meets the requirements of 10 CFR 73.55(b)(4) through (b)(11), and is, therefore, acceptable.*

13.6.4.1.4 Establishment of Security Organization

The provisions of 10 CFR 73.55(d) establish requirements to describe a security organization, including the management system for oversight of the physical protection program. The security organization must be designed, staffed, trained, qualified, re-qualified, and equipped to implement the physical protection program as required by 10 CFR 73.55(b) and 10 CFR Part 73, Appendices B and C.

Section 4.0 of the PSP describes how the applicant meets the requirements of 10 CFR 73.55(d)(1).

Security Organization Management

Section 4.1 of the PSP describes the organization's management structure. The PSP establishes that the security organization is a critical component of the physical protection program and is responsible for the effective application of engineered systems, technologies, programs, equipment, procedures, and personnel necessary to detect, assess, interdict, and neutralize threats up to and including the DBT of radiological sabotage. The security organization may be proprietary, contractor, or other qualified personnel.

The PSP describes that the organization will be staffed with appropriately trained and equipped personnel, in a command structure with administrative controls and procedures, to provide a comprehensive response. Section 4.1 of the PSP also describes the roles and responsibilities of the Security Organization. The PSP provides that at least one full-time, dedicated Security Shift Team Leader that has the authority for command and control of all security operations is onsite at all times.

The security force implementing the security functions as described in this section of the plan will be either a proprietary force, contractor, or other qualified personnel. The training qualification requirements are described in the T&QP.

The NRC staff has reviewed the applicant's description in PSP Sections 4 and 4.1 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the meets the requirements of 10 CFR 73.55(d) and is, therefore, acceptable.

The following portion of this technical evaluation section is reproduced from Section 13.6.4.1 of the VEGP SER:

*13.6.4.1.5 Qualification for Employment in Security*

*The requirements of 10 CFR 73.55(d)(3) state, in part, that the applicant may not permit any individual to implement any part of the physical protection program unless the individual has been trained, equipped and qualified to perform assigned duties and responsibilities in accordance with Appendix B to 10 CFR Part 73 and the applicant's T&QP.*

*Section 5 of the PSP describes that employment qualifications for members of the security force are delineated in the T&QP.*

*The NRC staff has reviewed the applicant's description in PSP Section 5 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the PSP meets the requirements of 10 CFR 73.55(d)(3), and is, therefore, acceptable.*

*13.6.4.1.6 Training of Facility Personnel*

*Consistent with requirements in 10 CFR 73.55(d)(3),10 CFR 73.56 and 10 CFR Part 73, Appendix B, Section VI.C.1, all personnel who are authorized unescorted access to the applicant's PA receive training, in part to ensure that they understand their role in security and their responsibilities in the event of a security incident. Individuals assigned to perform security-related duties or responsibilities, such as, but not limited to, material searches and vehicle escort are trained and qualified in accordance with the T&QP to perform these duties and responsibilities and to ensure that each individual has the minimum knowledge, skills, and abilities required for effective performance of assigned duties and responsibilities.*

*Section 6 of the PSP describes the training provided for all personnel who have been granted unescorted access to the applicant's PA.*

*The NRC staff has reviewed the applicant's description in PSP Section 6 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the PSP meets the requirements of 10 CFR 73.56 and 10 CFR Part 73, Appendix B, and is, therefore, acceptable.*

*13.6.4.1.7 Security Personnel Training*

*The provisions of 10 CFR 73.55(d) require that all security personnel are trained and qualified in accordance with 10 CFR Part 73, Appendix B, Section VI prior to performing their duties.*

*Section 7 of the PSP describes that all security personnel are trained, qualified and perform tasks at levels specific for their assignments in accordance with the applicant's T&QP.*

*The NRC staff has reviewed the applicant's description in PSP Section 7 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the PSP meets the requirements of 10 CFR 73.55(d), and is, therefore, acceptable. The NRC staff's review of the licensee T&QP is located in Section 13.6.4.2 of this SER.*

*13.6.4.1.8 Local Law Enforcement Liaison*

*The following requirement is stated in 10 CFR 73.55(k)(9) "To the extent practicable, licensees shall document and maintain current agreements with applicable law enforcement agencies to include estimated response times and capabilities." In addition, 10 CFR 73.55(m)(2) requires, in part, that an evaluation of the effectiveness of the physical protection system include an audit of response commitments by local, State and Federal law enforcement authorities.*

*Section 8 of the PSP provides a detailed discussion of its ongoing relationship with local law enforcement agencies (LLEAs). The plans addressing response, communication methodologies and protocols, command and control structures and marshaling locations are located in the operations procedures, emergency plan procedures and the site-specific law enforcement response plan. The law enforcement response plan is reviewed biennially concurrent with the PSP effectiveness review.*

*The NRC staff has reviewed the applicant's description in PSP Section 8 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the PSP meets the requirements of 10 CFR 73.55(k)(9) and 10 CFR 73.55(m)(2), and is, therefore, acceptable.*

13.6.4.1.9 Security Personnel Equipment

The requirements of 10 CFR 73.55(d)(3) state, in part, the applicant may not permit any individual to implement any part of the physical protection program unless the individual has been trained, equipped and qualified in accordance with 10 CFR Part 73, Appendix B and the T&QP. The provisions of 10 CFR Part 73, Appendix B, Section VI.G.2(a) state, in part, that the applicant must ensure that each individual is equipped or has ready access to all personal equipment or devices required for the effective implementation of the NRC-approved security plans, the applicant's protective strategy, and implementing procedures. The provisions of 10 CFR Part 73, Appendix B, Section VI.G.2(b) and (c) delineate the minimum equipment requirements for security personnel and armed response personnel.

Section 9 of the PSP describes the equipment, including armament, ammunition, and communications equipment that is provided to security personnel in order to ensure that security personnel are capable of performing the function stated in the Commission-approved security plans, applicant's protective strategy, and implementing procedures.

The NRC staff has reviewed the applicant's description in PSP Section 9 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the PSP meets the requirements of 10 CFR 73.55(d)(3) and Appendix B, Section VI.G.2, and is, therefore, acceptable.

The following portion of this technical evaluation section is reproduced from Section 13.6.4.1 of the VEGP SER:

> *13.6.4.1.10 Work Hour Controls*
>
> *The provisions of 10 CFR Part 26, "Fitness for Duty Programs," Subpart I, "Managing Fatigue," establish the requirements for managing fatigue. 10 CFR 26.205 establishes requirements for work hours. 10 CFR 26.205(a) requires that any individual who performs duties identified in 10 CFR 26.4(a)(1) through (a)(5) shall be subject to the requirements of this section.*
>
> *Section 10 of the PSP describes that the site will implement work hour controls consistent with 10 CFR Part 26, Subpart I, and that site procedures shall describe performance objectives and implementing procedures.*
>
> *The NRC staff's review of the fitness-for-duty program is found in Section 13.7 of this SER.*

13.6.4.1.11 Physical Barriers

The following requirements are established in 10 CFR 73.55(e): "Each applicant shall identify and analyze site-specific conditions to determine the specific use, type, function, and placement of physical barriers needed to satisfy the physical protection program design requirements of

10 CFR 73.55(b). (1) The applicant shall: (i) Design, construct, install and maintain physical barriers as necessary to control access into facility areas for which access must be controlled or denied to satisfy the physical protection program design requirements of paragraph (b) of this section." The regulation 10 CFR 73.55(b)(3)(ii) states, "Provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure the effectiveness of the physical protection program."

Section 11 of the PSP provides a general description of how the applicant has implemented its program for physical barriers, and that this implementation is in accordance with the performance objectives and requirements of 10 CFR 73.55(b).

Owner Controlled Area (OCA) Barriers

Section 11.1 of the PSP describes VCSNS use of OCA barriers at the site.

Vehicle Barriers

PSP Sections 11.2.1 and 11.2.2 establish and maintain vehicle control measures, as necessary, to protect against the DBT of radiological sabotage, consistent with the physical protection program design requirements of 10 CFR 73.55(b)(3)(ii) and 10 CFR 73.55(e)(10)(i), and in accordance with site-specific analysis. The PSP identifies measures taken to provide high assurance that such an event can be defended against. The applicant's PSP also provides that the inspection, monitoring, and maintenance of the vehicle barrier system (VBS) are included in the facility procedures.

Waterborne Threat Measures

The provisions of 10 CFR 73.55(e)(10)(ii) require the applicant to "Identify areas from which a waterborne vehicle must be restricted, and where possible, in coordination with local, State, and Federal agencies having jurisdiction over waterway approaches, deploy buoys, markers, or other equipment. In accordance with the site-specific analysis, provide periodic surveillance and observation of waterway approaches and adjacent areas."

Section 11.2.3 of the PSP describes that a site-specific analysis for a water-borne DBT has been conducted and documented. However, there is no waterborne access to VCSNS Units 2 and 3.

Protected Area Barriers

The provisions of 10 CFR 73.55(e)(8)(i) require that the protected area perimeter must be protected by physical barriers that are designed and constructed to: (1) limit access to only those personnel, vehicles, and materials required to perform official duties; (2) channel personnel, vehicles, and materials to designated access control portals; and (3) be separated from any other barrier designated as a vital area physical barrier, unless otherwise identified in the PSP.

The descriptions of the protected area (PA) barrier are provided in the PSP Section 11.3. These descriptions meet the definitions of physical barriers and protected areas in 10 CFR 73.2 and requirements of 10 CFR 73.55(e)(8).

In RAI 13.6-13, the NRC staff asked for a description of measures taken to ensure that detection, assessment, observation, and surveillance requirements of 10 CFR 73.55 are met and appropriate barriers are installed to prevent potential exploitation of structures and buildings whose walls and roofs comprise a portion of the PA.

In its response the applicant stated that the RAI 13.6-5 response from VEGP Units 3 and 4, dated October 16, 2009, is applicable to VCSNS Units 2 and 3. The VEGP Units 3 and 4 response to RAI 13.6-15 provided an explanation of measures that the applicant will take when a structure or building comprises a portion of the PA barrier.

On the basis of its review, the NRC staff finds the response to RAI 13.6-13 to be acceptable as it provides clarification on how the applicant meets requirements for describing where buildings or structures comprise a portion of the PA, consistent with 10 CFR 73.55(e)(10)(iv).

Section 11.3 of the PSP describes the extent to which the protected area barrier at the perimeter is separated from a vital area/island barrier. The security plan identifies where the PA barrier is not separated from a vital area barrier.

Section 11.3 of the PSP describes isolation zones. As required in 10 CFR 73.55(e)(7), the isolation zone is maintained in outdoor areas adjacent to the protected area perimeter barrier and is designed to ensure the ability to observe and assess activities on either side of the protected area perimeter.

Vital Area Barriers

The provisions of 10 CFR 73.55(e)(9) require that “Vital equipment must be located only within vital areas, which must be located within a protected area so that access to vital equipment requires passage through at least two physical barriers, except as otherwise approved by the Commission and identified in the security plans.” In addition, 10 CFR 73.55(e)(5) requires that certain vital areas shall be bullet resisting.

Section 11.4 of the PSP describes that vital areas are restricted access areas surrounded by physical barriers with the capability to restrict access to only authorized individuals. All vital areas are constructed in accordance with established regulatory requirements. Section 11.4 also describes that the reactor control room, central alarm station (CAS) and the location within which the last access control function for access to the protected area is performed, must be bullet resisting.

Target Set Equipment

The provisions of 10 CFR 73.55(f) require the following, “The licensee shall document and maintain the process used to develop and identify target sets, to include the site-specific analyses and methodologies used to determine and group the target set equipment or

elements. The licensee shall consider cyber attacks in the development and identification of target sets. Target set equipment or elements that are not contained within a protected or vital area must be identified and documented consistent with the requirements in § 73.55(f)(1) and be accounted for in the licensee's protective strategy. The licensee shall implement a process for the oversight of target set equipment and systems to ensure that changes to the configuration of the identified equipment and systems are considered in the licensee's protective strategy. Where appropriate, changes must be made to documented target sets."

Section 11.5 of the PSP describes that target set equipment or elements that are not contained within a protected or vital area are identified and accounted for in the site protective strategy.

The staff identified several RAIs relating to target sets for the purpose of reviewing the Westinghouse physical protection program. Westinghouse provided design details as background information to assist an applicant with the development of site-specific target set analyses. The staff evaluated the applicant's responses, and found them to be acceptable for the DC review of the AP1000 physical protection program. Westinghouse stated, in TR-94, APP-GW-GLR-066, "AP1000 Safeguards Assessment Report" that target sets were created to aid in the development of the AP1000 physical security system, and that final target sets will be developed by the COL applicant prior to fuel onsite (inside PA).

The NRC staff has reviewed the applicant's description in Sections 11.5 and 14.5 of the PSP, Section 7 of the SCP and information in Westinghouse TR-94, APP-GW-GLR-066, "AP1000 Safeguards Assessment Report" for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in Sections 11.5 and 14.5 of the PSP, Section 7 of the SCP and the information in Westinghouse TR-94 are consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the Sections 11.5 and 14.5 of the PSP and Section 7 of the SCP meets the requirements of 10 CFR 73.55(f)(1), (3), and (4), and is, therefore, acceptable. The target sets, target set analysis and site protective strategy are in the facility implementing procedures, which were not subject to an NRC staff review as part of this COL application, and are, therefore, subject to future NRC inspections in accordance with 10 CFR 73.55(c)(7)(iv) and 10 CFR Part 73, Appendix C, Section II.B.5(iii).

Delay Barriers

The provisions of 10 CFR 73.55(e)(3)(C)(ii) require that physical barriers must "provide deterrence, delay, or support access control" to perform the required function of the applicant physical protection program. The PSP describes the use of delay barriers at VCSNS Units 2 and 3.

Section 11.6 of the PSP includes a description of the use of Delay Barriers to meet requirement of 10 CFR 73.55(e).

The NRC staff has reviewed the applicant's description in PSP Sections 11, 11.1, 11.2, 11.2.1, 11.2.2, 11.2.3, and Sections 11.3 through 11.6 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800

acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the PSP meet the requirements of 10 CFR 73.55(e), and are, therefore, acceptable.

The following portion of this technical evaluation section is reproduced from Section 13.6.4.1 of the VEGP SER:

*13.6.4.1.12 Security Posts and Structures*

*The provisions of 10 CFR 73.55(e)(5) require that the reactor control room, the CAS, and the location within which the last access control function for access to the PA is performed, must be bullet-resisting.*

*Section 12 of the PSP describes that security posts and structures are qualified to a level commensurate with their application within the site protective strategy, and that these positions are constructed of bullet resisting materials.*

*The NRC staff has reviewed the applicant's description in PSP Section 12 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the PSP meets the requirements of 10 CFR 73.55(e)(5), and is, therefore, acceptable.*

*13.6.4.1.13 Access Control Devices*

*It is stated in 10 CFR 73.55(g)(1) that, consistent with the function of each barrier or barrier system, the applicant shall control personnel, vehicle, and material access, as applicable, at each access control point in accordance with the physical protection program design requirements of 10 CFR 73.55(b).*

*The provisions of 10 CFR 73.55(g)(6) require control of access control devices as stated: "The licensee shall control all keys, locks, combinations, passwords and related access control devices used to control access to protected areas, vital areas and security systems to reduce the probability of compromise."*

*<u>Types of Security-Related Access Control Devices</u>*

*Section 13.1 of the PSP describes that the applicant uses security-related access control devices to control access to protected and vital areas and security systems.*

*<u>Control and Accountability</u>*

*Section 13.2.1 of the PSP describes the control of security related locks. Section 13.2.2 of the PSP describes the controls associated with the changes to*

*and replacements of access control devices and the accountability and inventory control process, and the circumstances that require changes in security-related locks. The applicant uses facility procedures to produce, control, and recover keys, locks, and combinations for all areas and equipment, which serve to reduce the probability of compromise. The issue of access control devices is limited to individuals who have unescorted access authorization and require access to perform official duties and responsibilities. Keys and locks are accounted for through a key inventory control process as described in facility procedures.*

*The NRC staff has reviewed the applicant's description in PSP Sections 13, 13.1, 13.2, 13.2.1, and 13.2.2 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the PSP meet the requirements of 10 CFR 73.55(g)(1) and (6), and are, therefore, acceptable.*

13.6.4.1.14 Access Requirements

Access Authorization and Fitness for Duty

The provisions of 10 CFR 73.55(b)(7) require the applicant shall establish, maintain, and implement an access authorization program in accordance with 10 CFR 73.56 and shall describe the program in the PSP. The provisions of 10 CFR Part 26 require the applicant to establish and maintain a FFD program.

Section 14.1 of the PSP describes that the access authorization program implements regulatory requirements utilizing the provisions in RG 5.66.

The NRC staff has reviewed the applicant's description in PSP Section 14.1 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the PSP meets the requirements of 10 CFR 73.55(b)(7), 10 CFR 73.56 and 10 CFR Part 26 and is, therefore, acceptable.

Insider Mitigation Program

The provisions of 10 CFR 73.55(b)(9) require that the applicant shall establish, maintain, and implement an insider mitigation program and shall describe the program in the PSP. The insider mitigation program must monitor the initial and continuing trustworthiness and reliability of individuals granted or retaining unescorted access authorization to a protected or vital area, and implement defense-in-depth methodologies to minimize the potential for an insider to adversely affect, either directly or indirectly, the applicant's capability to prevent significant core damage and spent fuel sabotage. The insider mitigation program must include elements from: the access authorization program, the FFD program, the cyber security program and the physical protection program.

Section 14.2 of the PSP describes how the applicant will establish, maintain, and implement an insider mitigation program. The insider mitigation program requires elements from the access authorization program described in 10 CFR 73.56; FFD program described in 10 CFR Part 26; the cyber security program described in 10 CFR 73.54; and the physical security program described in 10 CFR 73.55. In addition, Section 14.2 describes the integration of the programs mentioned above to form a cohesive and effective insider mitigation program. The applicant addresses the observations for the detection of tampering. The NRC staff finds that this approach is an acceptable method for meeting the requirements 10 CFR 73.55(b)(9).

The NRC staff has reviewed the applicant's description in PSP Section 14.2 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the PSP meets the requirements of 10 CFR 73.55(b)(9) and is, therefore, acceptable.

Picture Badge Systems

Requirements for badges are stated in 10 CFR 73.55(g)(6)(ii). "The licensee shall implement a numbered photo identification badge system for all individuals authorized unescorted access to the protected area and vital areas." In addition, identification badges may be removed from the protected area under limited conditions and only by authorized personnel. Records of all badges shall be retained and shall include name and areas to which persons are granted unescorted access.

The provisions of 10 CFR 73.55(g)(7)(ii) require that individuals not employed by the applicant but who require frequent or extended unescorted access to the protected area and/or vital areas to perform duties and responsibilities required by the applicant at irregular or intermittent intervals, shall satisfy the access authorization requirements of 10 CFR 73.56 and 10 CFR Part 26 of this chapter, and shall be issued a non-employee photo identification badge that is easily distinguished from other identification badges before being allowed unescorted access to the protected and vital areas. Non-employee photo identification badges must visually reflect that the individual is a non-employee and that no escort is required.

Section 14.3 of the PSP describes the site picture badge system. Identification badges will be displayed while individuals are inside the protected area or vital areas. When not in use, badges may be removed from the protected area by authorized holders, provided that a process exists to deactivate the badge upon exit and positively confirm the individual's true identity and authorization for unescorted access prior to entry into the protected area. Records are maintained to include the name and areas to which unescorted access is granted of all individuals to whom photo identification badges have been issued.

The NRC staff has reviewed the applicant's description in PSP Section 14.3 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds

that the description provided in the PSP meets the requirements of 10 CFR 73.55(g)(6) and (7) and is, therefore, acceptable.

Searches

The provisions of 10 CFR 73.55(h) require, in part, that applicants meet the objective to detect, deter, and prevent the introduction of firearms, explosives, incendiary devices, or other items, which could be used to commit radiological sabotage. To accomplish this, applicant's shall search individuals, vehicles, and materials consistent with the physical protection program design requirements in paragraph (b) of this section, and the function to be performed at each access control point or portal before granting access.

Section 14.4 of the PSP provides an overview description of the search process for vehicle, personnel and materials. The search process is conducted using security personnel, specifically trained non-security personnel and technology. Detailed discussions of actions to be taken in the event unauthorized materials are discovered are found in implementing procedures.

Vehicle Barrier Access Control Point

The provisions of 10 CFR 73.55(h)(2)(ii) through (v) provide the requirements the applicant to search vehicles at the owner controlled area and 10 CFR 73.55(h)(3) provides requirements for searches of personnel, vehicles and materials prior to entering the protected area.

Section 14.4.1 of the PSP describes the process for the search of personnel, vehicles and materials at predetermined locations prior to granting access to designated facility areas identified by the applicant as needed to satisfy the physical protection program. The applicant states that it has developed specific implementing procedures to address vehicle and materials searches at these locations.

PA Packages and Materials Search

Section 14.4.2 of the PSP describes the process for conducting searches of packages and materials for firearms, explosives, incendiary devices, or other items, which could be used to commit radiological sabotage using equipment capable of detecting these items or through visual and physical searches, or both, to ensure that all items are clearly identified before these items can enter the VCSNS Units 2 and 3 protected area. Detailed requirements for conducting these searches are found in applicant implementing procedures and include the search and control of bulk materials and products. Applicant implementing procedures also discuss the control of packages and materials previously searched and tamper sealed by personnel trained in accordance with the T&QP.

PA Vehicle Search

Section 14.4.3 of the PSP describes the process for the search of vehicles for firearms, explosives, incendiary devices, or other items, which could be used to commit radiological sabotage using equipment capable of detecting these items or through visual and physical

searches, or both, to ensure that all items are clearly identified at the protected area. Detailed requirements for conducting these searches are found in the applicant's implementing procedures. The applicant's implementing procedures also address the search methodologies for vehicles that must enter the protected area under emergency conditions.

PA Personnel Searches

Section 14.4.4 of the PSP describes the process for searches of all personnel requesting access into protected areas. The PSP describes the search for firearms, explosives, incendiary devices, or other items, which could be used to commit radiological sabotage using equipment capable of detecting these items or through visual and physical searches or both to ensure that all items are clearly identified prior to granting access into the protected area. All persons except official Federal, State, and LLEA personnel on official duty are subject to these searches upon entry to the protected area. Detailed discussions of observation and control measures are found in implementing procedures.

PA Access Controls

Section 14.4.5 of the PSP describes the process for controlling access at all points where personnel or vehicles could gain access into the applicant's protected area. The plan notes that principal personnel access to the protected area is through a lockable portal. Personnel are only permitted into the PA after positive ID verification, access authorization verification, and a search is performed per Section 14.4 of the PSP. Vehicles are controlled through positive control methods described in the facility procedures.

Escort and Visitor Requirements

The provisions of 10 CFR 73.55(g)(7) state in part, that the applicant may permit escorted access to protected and vital areas to individuals who have not been granted unescorted access in accordance with the requirements of 10 CFR 73.56 and 10 CFR Part 26 of this chapter. 10 CFR 73.55(g)(8) discusses escort requirements. Applicants are required to implement procedures for processing, escorting and controlling visitors. Procedures shall address confirmation of identity of visitors, maintenance of a visitor control register, visitor badging and escort controls including, training, communications, and escort ratios.

Section 14.4.6 of the PSP describes the process for control of visitors. The PSP affirms that procedures address the identification, processing, and escorting of visitors and the maintenance of a visitor control register. Training requirements for escorting visitors includes responsibilities, communications and escort ratios. All escorts are trained to perform escort duties in accordance with site requirements. All visitors wear a badge that clearly indicates that an escort is required.

The NRC staff has reviewed the applicant's description in PSP Sections 14.4, and 14.4.1 through 14.4.6 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in NUREG-0800,

Section 13.6.1, the staff finds that the description provided in the PSP meets the requirements of 10 CFR 73.55(h)(2), (h)(3), (g)(7) and (g)(8), and are, therefore, acceptable.

Vital Area Access Controls

The provisions of 10 CFR 73.55(g)(4) require that applicants control access into vital areas consistent with established access authorization lists. In response to a site-specific credible threat or other credible information, applicants shall implement a two-person (line-of-sight) rule for all personnel in vital areas so that no one individual is permitted access to a vital area.

The provisions of 10 CFR 73.56(j) require the applicant to establish, implement, and maintain a list of individuals who are authorized to have unescorted access to specific nuclear power plant vital areas during non-emergency conditions. The list must include only those individuals who have a continued need for access to those specific vital areas in order to perform their duties and responsibilities. The list must be approved by a cognizant applicant manager or supervisor who is responsible for directing the work activities of the individual who is granted unescorted access to each vital area, and updated and re-approved no less frequently than every 31 days.

Section 14.5 of the PSP describes vital areas and states that the applicant maintains vital areas locked and protected by an active intrusion alarm system. An access authorization system is established to limit unescorted access that is controlled by an access authorization list which is reassessed and reapproved at least once every 31 days. Additional access control measures are described in the facility procedures.

The NRC staff has reviewed the applicant's description in PSP Section 14.5 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the PSP meets the requirements of 10 CFR 73.55(g)(4) and is, therefore, acceptable.

The following portion of this technical evaluation section is reproduced from Section 13.6.4.1 of the VEGP SER:

> *13.6.4.1.15 Surveillance Observation and Monitoring*
>
> *The provisions of 10 CFR 73.55(i)(1) require that the applicant establish and maintain intrusion detection systems that satisfy the design requirements of 10 CFR 73.55(b) and provide, at all times, the capability to detect and assess unauthorized persons and facilitate the effective implementation of the protective strategy.*
>
> *Illumination*
>
> *The provisions of 10 CFR 73.55(i)(6) require, in part, that all areas of the facility are provided with illumination necessary to satisfy the design requirements of 10 CFR 73.55(b) and implement the protective strategy. Specific requirements*

*include providing a minimum illumination level of 0.2 foot-candles, measured horizontally at ground level, in the isolation zones and appropriate exterior areas within the PA. Alternatively, the applicant may augment the facility illumination system by means of low-light technology to meet the requirements of this section or otherwise implement the protective strategy. The applicant shall describe in the security plans how the lighting requirements of this section are met and, if used, the type(s) and application of low-light technology.*

*Section 15.1 of the PSP describes that all isolation zones and appropriate exterior areas within the PA have lighting capabilities that provide illumination sufficient for the initiation of an adequate response to an attempted intrusion of the isolation zone, a PA, or a vital area. A discussion of the implementation of technology using fixed and non-fixed low light level cameras or alternative technological means is provided. The applicant has addressed the potential for loss of lighting and the compensatory actions that would be taken if that event were to occur.*

*Surveillance Systems*

*The provisions of 10 CFR 73.55(i)(1) require, in part, that the applicant implement, establish, and maintain intrusion detection and assessment, surveillance, observation and monitoring systems to satisfy the design requirements of 10 CFR 73.55(b), and of the applicant's OCA.*

*Section 15.2 of the PSP describes that surveillance is accomplished by human observation and technology. Surveillance systems include a variety of cameras, video display, and annunciation systems designed to assist the security organization in observing, detecting assessing alarms or unauthorized activities. Certain systems provide real-time and recorded play back of recorded video images. The specifics of surveillance systems are described in facility implementing procedures.*

*Intrusion Detection Equipment*

*Section 15.3 of the PSP describes the perimeter intrusion detection system, and the PA and vital area intrusion detection systems. These systems are capable of detecting attempted penetration of the PA perimeter barrier; are monitored with assessment equipment designed to satisfy the requirements of 10 CFR 73.55(i) and provide real-time and play-back/recorded video images of the detected activities before and after each alarm annunciation. The PSP describes how the applicant will meet regulatory requirements for redundancy, tamper indication and uninterruptable power supply.*

*Central Alarm Station (CAS) and Secondary Alarm Station (SAS) Operation*

*The provisions of 10 CFR 73.55(i)(4) provide requirements for alarm stations. It is required, in 10 CFR 73.55(i)(4)(i), that both alarm stations must be designed*

*and equipped to ensure that a single act, in accordance with the DBT of radiological sabotage defined in 10 CFR 73.1, cannot disable both alarm stations. The applicant shall ensure the survivability of at least one alarm station to maintain the ability to perform the following functions: 1) detect and assess alarms; 2) initiate and coordinate an adequate response to an alarm; 3) summon offsite assistance; and 4) provide command and control. 10 CFR 73.55(i)(4)(iii) requires that alarm stations must be equal and redundant.*

*Section 15.4 of the PSP describes the functional operations of the CAS and the SAS. The PSP provides that the alarm stations are equipped, such that no single act will disable both alarm stations. The applicant's PSP provides that each alarm station is properly manned and that no activities are permitted that would interfere with the operator's ability to execute assigned duties and responsibilities.*

*Security Patrols*

*Owner Controlled Area (OCA) Surveillance and Response*

*The provisions of 10 CFR 73.55(e)(6) require that the applicant establish and maintain physical barriers in the OCA as needed to satisfy the physical protection program design requirements of 10 CFR 73.55(b). It is required, in 10 CFR 73.55(i)(5)(ii), in part, that the applicant provide continuous surveillance, observation and monitoring of the OCA and that these responsibilities may be performed by security personnel during continuous patrols, through the use of video technology, or by a combination of both.*

*Section 15.5.1 of the PSP describes the processes used to meet this requirement. The PSP discusses the process to be used and provides that details regarding the implementation of OCA surveillance techniques are found in facility procedures. The PSP provides a discussion regarding the implementation of manned and video options for patrolling and surveillance of the OCA.*

*Protected and Vital Area Patrols*

*The provisions of 10 CFR 73.55(i)(5)(iii) through (viii) require, in part, that armed patrols check unattended openings that intersect a security boundary, such as an underground pathways, check external areas of the PA and vital area portals, periodically inspect vital areas, conduct random patrols of accessible target set equipment, be trained to recognize obvious tampering and if detected, initiate an appropriate response in accordance with established plans and procedures.*

*Section 15.5.2 of the PSP describes the process employed by the applicant to meet the above requirements. The PSP describes the areas of the facility that will be patrolled and observed, as well as the frequency of these patrols and observations. The applicant has addressed the observations for the detection of tampering in Section 14.2 of the PSP and in the facility procedures.*

*The NRC staff has reviewed the applicant's description in PSP Sections 15, 15.1 through 15.4, 15.5.1, and 15.5.2 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the PSP meets the requirements of 10 CFR 73.55(b) and (i), and are, therefore, acceptable.*

*13.6.4.1.16 Communications*

*The provisions of 10 CFR 73.55(j)(1) through (6) describe the requirements for establishment and maintenance of continuous communication capabilities with both onsite and offsite resources to ensure effective command and control during both normal and emergency situations. Alarm stations must be capable of calling for assistance, on-duty security force personnel must be capable of maintaining continuous communication with each alarm station and vehicle escorts, and personnel escorts must maintain timely communication with security personnel. Continuous communication capabilities must terminate in both alarm stations, between LLEA and the control room. Non-portable communications must remain operable from independence power sources. The applicant must identify areas where communications could be interrupted or not maintained.*

*Notifications (Security Contingency Event Notifications)*

*Section 16.1 of the PSP describes that the applicant have a process to ensure that continuous communications are established and maintained between the onsite security force staff and the offsite support agencies.*

*System Descriptions*

*Section 16.2 of the PSP describes the establishment and maintenance of the communications system. Detailed descriptions of security systems are included in the facility procedures. VEGP has access to both hard wired and alternate communications systems. Site security personnel are assigned communications devices with which to maintain continuous communications with the CAS and SAS. All personnel and vehicles are assigned communications resources with which to maintain continuous communications. Continuous communication protocols are available between the CAS, SAS and the control room.*

*The NRC staff has reviewed the applicant's description in PSP Sections 16, 16.1 and 16.2 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the PSP meets the requirements of 10 CFR 73.55(j)(1) through (6), and are, therefore, acceptable.*

*13.6.4.1.17 Review, Evaluation and Audit of the Physical Security Program*

*The provisions of 10 CFR 73.55(m) require, in part, that each element of the physical protection program will be reviewed at least every 24 months. An initial review is required within 12 months after original plan implementation, or a change in personnel, procedures, equipment or facilities, which could have a potentially adverse affect on security, or as necessary based on site-specific analysis assessments, or other performance indicators. Reviews must be conducted by individuals independent of the security program and must include the plans, implementing procedures and local law enforcement commitments. Results of reviews shall be presented to senior management above the level of the security manager and findings must be entered in the site corrective action program.*

*Section 17 of the PSP describes that the physical security program is reviewed 12 months following initial implementation and at least every 24 months by individuals independent of both security program management and personnel who have a direct responsibility for implementation of the security program. The physical security program review includes, but is not limited to, an audit of the effectiveness of the physical security program, cyber security plans, implementing procedures, safety/security interface activities, the testing, maintenance, and calibration program, and response commitments by local, State, and Federal law enforcement authorities.*

*A review shall be conducted as necessary based upon site-specific analyses, assessments, or other performance indicators and as soon as reasonably practical, but no longer than 12 months, after changes occur in personnel, procedures, equipment, or facilities that potentially could adversely affect safety/security.*

*The results and recommendations of the physical security program review, management's finding on whether the physical security program is currently effective and any actions taken as a result of recommendations from prior program reviews are documented in a report to plant management and to appropriate corporate management at least one level higher than that having responsibility for the day-to-day plant operation. These reports are maintained in an auditable form and maintained for inspection.*

*Findings from the onsite physical security program reviews are entered into the facility corrective action program.*

*In RAI 13.6-36, the NRC staff requested that the applicant address the requirements of 10 CFR 73.58, "Safety/security requirements for nuclear power reactors." In its response dated May 14, 2010, the applicant stated that management controls and processes used to establish and maintain an effective interface between nuclear safety and physical security are addressed by*

*administrative procedures. The applicant committed to revise VEGP COL FSAR Section 13.5.1 to include the safety/security interface implementation process in the list of procedural instructions provided in plant administrative procedures.*

*On the basis of its review, the NRC staff finds that since the applicant will revise VEGP COL FSAR Section 13.5.1 to incorporate the requirements for safety/security interfaces, the response to RAI 13.6-36 meets the requirements of 10 CFR 73.58 and is, therefore, acceptable. The incorporation of changes to the VEGP COL FSAR Section 13.5.1 is being tracked as* ***Confirmatory Item 13.6-2****.*

*The NRC staff has reviewed the applicant's description in PSP Section 17 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the PSP meets the requirements of 10 CFR 73.55(m), and is, therefore, acceptable.*

13.6.4.1.18 Response Requirements

The provisions of 10 CFR 73.55(k) require, in part, that the applicant establish and maintain a properly trained, qualified, and equipped security force required to interdict and neutralize threats up to and including the DBT defined in 10 CFR 73.1, to prevent significant core damage and spent fuel sabotage. To meet this objective, the applicant must ensure that necessary equipment is in supply, working, and readily available. The applicant must ensure training has been provided to all armed members of the security organization who will be available onsite to implement the applicant's protective strategy as described in the facility procedures and 10 CFR Part 73, Appendix C. The applicant must have facility procedures to reconstitute armed response personnel and have established working agreement(s) with LLEA. The applicant must have implemented a threat warning system to accommodate heightened security threats and coordination with NRC representatives.

Section 18 of the PSP describes an armed response team, responsibilities, training, and equipment, and requires an adequate number of armed response force personnel immediately available at all times to implement each site's protective strategy. The applicant ensures that training is conducted in accordance with the requirements of 10 CFR Part 73, Appendix B that will ensure implementation of the site protective strategy in accordance with 10 CFR Part 73, Appendix C. Procedures are in place to reconstitute the armed response personnel as are agreements with LLEA. Procedures are in place to manage the threat warning system.

The NRC staff has reviewed the applicant's description in PSP Section 18 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the PSP meets the requirements of 10 CFR 73.55(k) and is, therefore, acceptable.

The following portion of this technical evaluation section is reproduced from Section 13.6.4.1 of the VEGP SER:

*13.6.4.1.19 Special Situations Affecting Security*

*The provisions of 10 CFR 73.58 require that each operating nuclear power reactor applicant with a license issued under 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities" or 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants" shall comply with the following requirements: the applicant shall assess and manage the potential for adverse effects on safety and security, including the site emergency plan, before implementing changes to plant configurations, facility conditions, or security; the scope of changes to be assessed and managed must include planned and emergent activities (such as, but not limited to, physical modifications, procedural changes, changes to operator actions or security assignments, maintenance activities, system reconfiguration, access modification or restrictions, and changes to the security plan and its implementation); where potential conflicts are identified, the applicant shall communicate them to appropriate personnel and take compensatory and/or mitigative actions to maintain safety and security under applicable Commission regulations, requirements, and license conditions.*

*Section 19 of the PSP includes requirements for assessments to manage increased risk of special situations affecting security.*

*<u>Refueling/Major Maintenance</u>*

*Section 19.1 of the PSP describes that, for refueling or major maintenance activities, the PSP describes that security procedures identify measures for implementation of actions prior to refueling or major maintenance activities. These measures include controls to ensure that a search is conducted prior to revitalizing an area, that protective barriers and alarms are fully operational, and post-maintenance performance testing to ensure operational readiness of equipment in accordance with 10 CFR 73.55(n)(8).*

*<u>Construction and Maintenance</u>*

*Section 19.2 of the PSP describes that during periods of construction and maintenance when temporary modifications are necessary, that the applicant will implement measures that provide for equivalency in the physical protective measures and features impacted by the activities, such that physical protection measures are not degraded. The process for making such changes or modifications is included in the facility procedures.*

*The NRC staff has reviewed the applicant's description in PSP Sections 19, 19.1, and 19.2 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance*

*criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the PSP meets the requirements of 10 CFR 73.55(n)(8) and 10 CFR 73.58, and are, therefore, acceptable.*

*13.6.4.1.20 Maintenance, Testing and Calibration*

*In accordance with 10 CFR 73.55(n), the applicant is required to establish, maintain, and implement a maintenance, testing, and calibration program to ensure that security systems and equipment, including secondary and uninterruptible power supplies, are tested for operability and performance at predetermined intervals, maintained in operable condition, and have the capability of performing their intended functions. The regulation requires that the applicant describe their maintenance testing and calibrations program in the PSP, and that the implementing procedures describe the details and intervals for conducting these activities. Applicant procedures must identify criteria for documenting deficiencies in the corrective action program and ensuring data protection in accordance with 10 CFR 73.21. The applicant must conduct periodic operability testing of the intrusion alarm system and must conduct performance testing in accordance with the PSP and implementing procedures. Communication equipment must be tested not less than daily, and search equipment must also be tested periodically. Procedures must be established for testing equipment located in hazardous areas, and procedures must be established for returning equipment to service after each repair.*

*Sections 20.1 through 20.6 of the PSP describe the maintenance, testing and calibration program for security-related equipment. Section 20.1 states that the applicant shall conduct intrusion detection testing in accordance with recommended testing procedures described in RG 5.44," Perimeter Intrusion Alarm System". Each operational component required for the implementation of the security program is at a minimum, tested in accordance with 10 CFR 73.55(n), the PSP and implementing procedures.*

*The NRC staff has reviewed the applicant's description in PSP Section 20 and 20.1 through 20.6 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the PSP meets the requirements of 10 CFR 73.55(n), and are, therefore, acceptable.*

*13.6.4.1.21 Compensatory Measures*

*The provisions of 10 CFR 73.55(o) require, in part, that the applicant shall identify criteria and measures to compensate for degraded or inoperable equipment, systems, and components to meet the requirements of this section. Compensatory measures must provide a level of protection that is equivalent to the protection that was provided by the degraded or inoperable, equipment,*

*system, or components. Compensatory measures must be implemented within specific time frames necessary to meet the appropriate portions of 10 CFR 73.55(b) and described in the security plans.*

*Section 21 of the PSP identifies measures and criteria required to compensate for degraded or inoperable equipment, systems, and components in accordance with 10 CFR 73.55(o) to assure that the effectiveness of the physical protection system is not reduced by failure or other contingencies affecting the operation of the security-related equipment or structures. Sections 21.1 through 21.12 of the PSP address PA and vital area barriers, intrusion detection and alarm systems, lighting, fixed and non-fixed closed circuit television, play-back and recorded video systems, computer systems, access control devices, vehicle barrier systems, channeling barrier systems, and other security-related equipment.*

*The NRC staff has reviewed the applicant's description in PSP Sections 21 and 21.1 through 21.12, for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the PSP meets the requirements of 10 CFR 73.55(o), and are, therefore, acceptable.*

*13.6.4.1.22 Records*

*The provisions of 10 CFR Part 26, 10 CFR 73.55(q), 10 CFR 73.56(k) and (o), 10 CFR Part 73, Appendix B. Section VI.H., Appendix C, Section II.C and 10 CFR 73.70, require that the applicant must retain and maintain all records required to be kept by the Commission regulations, orders, or license conditions until the Commission terminates the license for which the records were developed, and shall maintain superseded portions of these records for at least three years after the record is superseded, unless otherwise specified by the Commission. The applicant is required to keep records of contracts with any contracted security force that implements any portion of the onsite physical protection program for the duration of the contract. The applicant must make all records, required to be kept by the Commission, available to the Commission and the Commission may inspect, copy, retain and remove all such records, reports and documents, whether kept by the applicant or a contractor. Review and audit reports must be maintained and available for inspection for a period of three years.*

*Section 22.0 of the PSP addresses the requirements to maintain records. Sections 22.1 through 22.13 address each kind of record that the applicant will maintain and the duration of retention for each record. The following types of records are maintained in accordance with the above mention regulations: access authorization records; suitability, physical and psychological qualification records for security personnel; PA and vital area access control records; PA visitor access records; PA vehicle access; vital area access transaction records;*

*vitalization and de-vitalization records; vital area access list reviews; security plans and procedures; security patrols, inspections and tests; maintenance; CAS and SAS alarm annunciation and security response records; local law enforcement agency records; records of audits and reviews; access control devices; security training and qualification records; firearms testing and maintenance records; and engineering analysis for the vehicle barrier system.*

*The NRC staff has reviewed the applicant's description in PSP Sections 22 and 22.1 through 22.13 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the PSP meets the requirements of 10 CFR 73.55(q), 10 CFR 73.55(o) and 10 CFR 73.70, and are, therefore, acceptable.*

*13.6.4.1.23 Digital Systems Security*

*Section 23 of the PSP addresses digital systems security. The applicant stated in its PSP that it has implemented the requirements of 10 CFR 73.54 and maintains a cyber security plan that describes how it has provided high assurance that safety, security, and emergency preparedness functions are protected against the DBT.*

*The NRC staff's review of the cyber security plan is found Section 13.8 of this SER.*

*13.6.4.1.24 Temporary Suspension of Security Measures*

*The provisions of 10 CFR 73.55(p) allow the applicant to "suspend implementation of affected requirements of this section under the following conditions: In accordance with 10 CFR 50.54(x) and 50.54(y) of this chapter, the licensee may suspend any security measures under this section in an emergency when this action is immediately needed to protect the public health and safety and no action consistent with license conditions and technical specifications that can provide adequate or equivalent protection is immediately apparent. This suspension of security measures must be approved as a minimum by a licensed senior operator before taking this action. During severe weather when the suspension of affected security measures is immediately needed to protect the personal health and safety of security force personnel and no other immediately apparent action consistent with the license conditions and technical specifications can provide adequate or equivalent protection. This suspension of security measures must be approved, as a minimum, by a licensed senior operator, with input from the security supervisor or manager, before taking this action."*

*Suspension of Security Measures in Accordance with 10 CFR 50.54(x) and (y)*

*Section 24.1 of the PSP addresses suspension of security measures in accordance with 10 CFR 50.54(x) and 10 CFR 50.54(y). Specifically, the plan provides a description of the conditions under which suspension is permissible, the authority for suspension, and the requirements for reporting such a suspension.*

*Suspension of Security Measures during Severe Weather or Other Hazardous Conditions*

*As required in 10 CFR 73.55(p), suspension of security measures are reported and documented in accordance with the provisions of 10 CFR 73.71. This suspension of security measures must be approved, as a minimum, by a licensed senior operator, with input from the security supervisor or manager, before taking this action. Suspended security measures must be reinstated as soon as conditions permit.*

*Section 24.2 of the PSP provides that certain security measures may be temporarily suspended during circumstances such as imminent, severe or hazardous weather conditions, but only when such action is immediately needed to protect the personal health and safety of security force personnel and no other immediately apparent action consistent with the security measures can provide adequate or equivalent protection. Under the PSP, suspended security measures shall be restored as soon as practical.*

*The NRC staff has reviewed the applicant's description in PSP Sections 24, 24.1, and 24.2 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the PSP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the PSP meets the requirements of 10 CFR 73.55(p), and are, therefore, acceptable.*

*13.6.4.1.25 Appendix A Glossary of Terms and Acronyms*

*Appendix A, "Glossary of Terms and Acronyms," was reviewed and found to be consistent with the NRC endorsed NEI 03-12, Revision 6 template.*

*13.6.4.1.26 Conclusions on the Physical Security Plan*

*On the basis of the NRC staff's review described in Sections 13.6.4.1.1 through 13.6.4.1.25 of this SER, the PSP meets the requirements of 10 CFR 73.55(a) through (r). The target sets, Target Set Analysis and Site Protective Strategy are in the facility implementing procedures, which were not subject to NRC staff review as part of this COL application and are, therefore, subject to future NRC inspection in accordance with 10 CFR 73.55(c)(7)(iv) and*

*10 CFR Part 73, Appendix C, Section II.B.5(iii). The NRC staff concludes that complete and procedurally correct implementation of the PSP will provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.*

*13.6.4.2 Appendix B Training and Qualification Plan*

*13.6.4.2.1 Introduction*

*The provisions of 10 CFR 73.55(c)(4) state that the applicant establish, maintain, implement, and follow a T&QP that describes how the criteria set forth in 10 CFR Part 73, Appendix B will be implemented.*

*The provisions of 10 CFR 73.55(d)(3) state that the applicant may not permit any individual to implement any part of the physical protection program unless the individual has been trained, equipped, and qualified to perform their assigned duties and responsibilities in accordance with 10 CFR Part 73, Appendix B and the T&QP. Non-security personnel may be assigned duties and responsibilities required to implement the physical protection program and shall:*

*(i) Be trained through established applicant training programs to ensure each individual is trained, qualified, and periodically requalified to perform assigned duties.*

*(ii) Be properly equipped to perform assigned duties.*

*(iii) Possess the knowledge, skills, and abilities to include physical attributes, such as sight and hearing, required to perform their assigned duties and responsibilities.*

*In addition, 10 CFR Part 73, Appendix B, Section VI.D.2(a) states armed and unarmed individuals shall be requalified at least annually in accordance with the requirements of the Commission-approved T&QP.*

*The T&QP describes that it is written to address the requirements found in 10 CFR Part 73, Appendix B, Section VI. The objective of the plan is to provide a mechanism to ensure that members of the security organization, and all others who have duties and responsibilities in implementing the security requirements and protective strategy, are properly trained, equipped and qualified. Deficiencies identified during the administration of T&QP requirements are documented in the site corrective action program.*

*The NRC staff has reviewed the introduction section in the T&QP and has determined that it includes all of the programmatic elements necessary to satisfy the requirements of 10 CFR 73.55 and 10 CFR Part 73, Appendix B, Section VI*

*applicable to the T&QP. Additional section-by-section evaluations and discussions are found in the following paragraphs.*

*13.6.4.2.2 Employment Suitability and Qualification*

*The requirements for mental qualifications, documentation, and physical requalification for security personnel (applicant employee and contractor) are described in the following T&QP sections.*

*Suitability*

*The provisions of 10 CFR Part 73, Appendix B, Section VI.B.1(a) require, in part, that before employment, or assignment to the security organization, an individual shall: (1) possess a high school diploma or pass an equivalent performance examination designed to measure basic mathematical, language, and reasoning skills, abilities, and knowledge required to perform security duties and responsibilities; (2) attained the age of 21 for an armed capacity or the age of 18 for an unarmed capacity; (3) not have any felony convictions that reflect on the individual's reliability; and (4) individuals in an armed capacity would not be disqualified from possessing or using firearms or ammunition in accordance with applicable State or Federal law, to include 18 U.S.C. 922. Applicants shall use information that has been obtained during the completion of the individual's background investigation for unescorted access to determine suitability. Satisfactory completion of a firearms background check for the individual under 10 CFR 73.19 of this part will also fulfill this requirement. The provisions of 10 CFR Part 73, Appendix B, Section VI.B.1(b) require the qualification of each individual to perform assigned duties and responsibilities must be documented by a qualified training instructor and attested to by a security supervisor.*

*Section 2.1 of the T&QP details the requirements of qualifications for employment in the security organization that follows the regulation in 10 CFR Part 73, Appendix B, Section VI.B.1(a).*

*Physical Qualifications*

*The provisions of 10 CFR Part 73, Appendix B, Section VI.B.2 require, in part, that individuals whose duties and responsibilities are directly associated with the effective implementation of the Commission-approved security plans, applicant protective strategy, and implementing procedures, may not have any physical conditions that would adversely affect their performance of assigned security duties and responsibilities.*

*Section 2.2 of the T&QP details those individuals that are directly associated with implementation of the security plans. Protective strategy and procedures may not have any physical conditions that would adversely affect their performance of assigned security duties and responsibilities. All individuals that are found on the*

*critical task matrix shall demonstrate the necessary physical qualifications prior to duty.*

*Physical Examination*

*It is stated in 10 CFR Part 73, Appendix B, Section VI.B.2(a)(2), that armed and unarmed individuals assigned security duties and responsibilities shall be subject to a physical examination designed to measure the individual's physical ability to perform assigned duties and responsibilities as identified in the Commission-approved security plans, applicant protective strategy, and implementing procedures.*

*The provisions of 10 CFR Part 73, Appendix B, Section VI.B.2(a)(3) state, in part, that the physical examination must be administered by a licensed health professional with the final determination being made by a licensed physician to verify the individual's physical capability to perform assigned duties and responsibilities.*

*The provisions of 10 CFR Part 73, Appendix B, Section VI.B.2(a)(4)(b) through (e) provide the minimum requirements that individuals must meet, and include requirements for vision, hearing, review of existing medical conditions, and examination for potential addictions.*

*The provisions of 10 CFR Part 73, Appendix B, Section VI.B.2(f) address medical examinations before returning to assigned duties following any incapacitation.*

*Section 2.3 of the T&QP describes the physical examinations for armed and unarmed individuals assigned security duties, as well as other individuals that implement parts of the physical protection program. Minimum requirements exist for physical examinations of vision, hearing, existing medical conditions, addiction or other physical requirements.*

*The NRC staff has reviewed the applicant's description in T&QP Sections 2.1, 2.2, and 2.3 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the T&QP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the T&QP meets the requirements of 10 CFR Part 73 Appendix B, Sections VI.B.1 and VI.B.2, and are, therefore, acceptable.*

*Medical Examinations and Physical Fitness Qualifications*

*The provisions of 10 CFR Part 73, Appendix B, Section VI.B.4(a) require, in part, that armed members of the security organization shall be subject to a medical examination by a licensed physician, to determine the individual's fitness to participate in physical fitness tests, and that the applicant shall obtain and retain*

*a written certification from the licensed physician that no medical conditions were disclosed by the medical examination that would preclude the individual's ability to participate in the physical fitness tests or meet the physical fitness attributes or objectives associated with assigned duties.*

*The provisions of 10 CFR Part 73, Appendix B, Section VI.B.4(b) require, in part, that before assignment, armed members of the security organization shall demonstrate physical fitness for assigned duties and responsibilities by performing a practical physical fitness test. The physical fitness test must consider physical conditions such as strenuous activity, physical exertion, levels of stress, and exposure to the elements as they pertain to each individual's assigned security duties. The physical fitness qualification of each armed member of the security organization must be documented by a qualified training instructor and attested to by a security supervisor.*

*Section 2.4 of the T&QP is explicit in its requirements for medical examinations and physical qualifications.*

*The NRC staff has reviewed the applicant's description in T&QP Section 2.4 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the T&QP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the T&QP meets the requirements of 10 CFR Part 73, Appendix B, Section VI.B.4(a) and 10 CFR Part 73, Appendix B, Section VI.B.4(b), and is, therefore, acceptable.*

*Psychological Qualifications*

*General Psychological Qualifications*

*The provisions of 10 CFR Part 73, Appendix B, Section VI.B.3(a) require, in part, that armed and unarmed individuals shall demonstrate the ability to apply good judgment, mental alertness, the capability to implement instructions and assigned tasks, and possess the acuity of senses and ability of expression sufficient to permit accurate communication by written, spoken, audible, visible, or other signals required by assigned duties and responsibilities.*

*Section 2.5.1 of the T&QP details that individuals whose security tasks and jobs directly associated with the effective implementation of the security plan and protective strategy shall demonstrate the qualities in 10 CFR Part 73, Appendix B, Section VI.B.3(a).*

*Professional Psychological Examination*

*The provisions of 10 CFR Part 73, Appendix B, Section VI.B.3(b) require, in part, that a licensed psychologist, psychiatrist, or physician trained in part to identify*

*emotional instability shall determine whether armed members of the security organization and alarm station operators in addition to meeting the requirement stated in paragraph (a) of this section, have no emotional instability that would interfere with the effective performance of assigned duties and responsibilities.*

*The provisions of 10 CFR Part 73, Appendix B, Section VI.B.3(c) require that a person professionally trained to identify emotional instability shall determine whether unarmed individuals, in addition to meeting the requirement stated in paragraph (a) of this section, have no emotional instability that would interfere with the effective performance of assigned duties and responsibilities.*

*Section 2.5.2 of the T&QP provides for the administration of psychological and emotional determination that will be conducted by appropriately licensed and trained individuals.*

*The NRC staff has reviewed the applicant's description in T&QP Sections 2.5.1 and 2.5.2 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the T&QP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the T&QP meets the requirements of 10 CFR Part 73, Appendix B, Sections VI.B.3(a), (b) and (c), and are, therefore, acceptable.*

*Documentation*

*The provisions of 10 CFR Part 73, Appendix B, Section VI.H.1 require, in part, the retention of all reports, records, or other documentation required by Appendix B and 10 CFR 75.55(q).*

*Section 2.6 of the T&QP describes that qualified training instructors create the documentation of training activities and that security supervisors attest to these records as required. Records are retained in accordance with Section 22 of the PSP.*

*The NRC staff has reviewed the applicant's description in T&QP Section 2.6 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the T&QP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the T&QP meets the requirements of 10 CFR Part 73, Appendix B, Section VI.H.1 and is, therefore, acceptable.*

*Physical Requalification*

*The provisions of 10 CFR Part 73, Appendix B, Section VI.B.5 require that: (a) at least annually, armed and unarmed individuals shall be required to demonstrate the capability to meet the physical requirements of this appendix and the*

*applicant's T&QP; and (b) the physical requalification of each armed and unarmed individual must be documented by a qualified training instructor and attested to by a security supervisor.*

*Section 2.7 of the T&QP describes that physical requalification is conducted at least annually, and documented as described in the PSP.*

*The NRC staff has reviewed the applicant's description in T&QP Section 2.7 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the T&QP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the T&QP meets the requirements of 10 CFR Part 73, Appendix B, Section VI.B.5 and is, therefore, acceptable.*

13.6.4.2.3 Individual Training and Qualification

Duty Training

The provisions of 10 CFR Part 73, Appendix B, Section VI.C.1 provide for duty training and qualification requirements. The regulation states, in part, that all personnel who are assigned to perform any security-related duty or responsibility shall be trained and qualified to perform assigned duties and responsibilities to ensure that each individual possesses the minimum knowledge, skills, and abilities required to effectively carry out those assigned duties and responsibilities. These areas of training include performing assigned duties and responsibilities in accordance with the requirements of the T&QP and the PSP, and be trained and qualified in the use of all equipment or devices required to effectively perform all assigned duties and responsibilities.

Section 3.1 of the T&QP details the requirements that individuals assigned duties must be trained in their duties, meet minimum qualifications, and be trained and qualified in all equipment or devices required to perform their duties.

The NRC staff has reviewed the applicant's description in T&QP Sections 3.0 and 3.1 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the T&QP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the T&QP meets the requirements of 10 CFR Part 73, Appendix B, Section VI.C.1, and is, therefore, acceptable.

On-the-job Training

The provisions of 10 CFR Part 73, Appendix B, Sections VI.C.2(a) through (c) provides requirements for on-the-job training. On-the-job training must include individual demonstration of the knowledge, skills and abilities provided during the training process. Individuals assigned contingency duties must complete a minimum of 40 hours of on-the-job training.

On-the-job training for contingency activities and drills must include, but is not limited to, hands-on application of knowledge, skills, and abilities related to: (1) response team duties; (2) use of force; (3) tactical movement; (4) cover and concealment; (5) defensive positions; (6) fields-of-fire; (7) re-deployment; (8) communications (primary and alternate); (9) use of assigned equipment; (10) target sets; (11) table top drills; (12) command and control duties; (13) applicant's protective strategy.

The T&QP provides a comprehensive discussion of the applicant's approach to meeting the requirements for on-the-job training.

The NRC staff has reviewed the applicant's description in T&QP Section 3.2 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the T&QP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the T&QP meets the requirements of 10 CFR Part 73, Appendix B, Sections VI.C.2(a) through (c), and is, therefore, acceptable.

Critical Task Matrix

The provisions of 10 CFR Part 73, Appendix B, Section VI.C.2(b) require, in part, that each individual who is assigned duties and responsibilities identified in the Commission-approved security plans, licensee protective strategy, and implementing procedures shall, before assignment, demonstrate proficiencies in implementing the knowledge, skills and abilities to perform assigned duties.

The T&QP includes a critical task matrix as Table 1 of the T&QP. This matrix addresses the means through which each individual will demonstrate the required proficiencies. Tasks that individuals must perform are listed in RG 5.75.

The NRC staff has reviewed the applicant's description in T&QP Section 3.3 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the T&QP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the T&QP meets the requirements of 10 CFR Part 73, Appendix B, Section VI.C.2(b), and is, therefore, acceptable.

Initial Training and Qualification Requirements

The provisions of 10 CFR Part 73, Appendix B, Sections VI.C.1(a) through (b) provide the requirements for duty training.

The provisions of 10 CFR Part 73, Appendix B, Section VI.D.1(a) provide the requirements for demonstration of qualification.

Section 3.4 of the T&QP details that individuals are trained and qualified prior to performing security-related duties within a security organization and must meet the minimum qualifying standards in Sections 3.4.1 and 3.4.2.

Written Examination

The provisions of 10 CFR Part 73, Appendix B, Section VI.D.1(b)(1) provide that written exams must include those elements listed in the Commission-approved T&QP to demonstrate an acceptable understanding of assigned duties and responsibilities, to include the recognition of potential tampering involving both safety and security equipment and systems.

Hands on Performance Demonstration

The provisions of 10 CFR Part 73, Appendix B, Section VI.D.1(b)(2) require that armed and unarmed individuals shall demonstrate hands-on performance for assigned duties and responsibilities by performing a practical hands-on demonstration for required tasks. The hands-on demonstration must ensure that theory and associated learning objectives for each required task are considered and each individual demonstrates the knowledge, skills, and abilities required to effectively perform the task.

Sections 3.4.1 and 3.4.2 of the T&QP describe the measures that are implemented by the applicant that meet the requirements stated above.

The NRC staff has reviewed the applicant's description in T&QP Sections 3.4, 3.4.1, and 3.4.2 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the T&QP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the T&QP meets the requirements of 10 CFR Part 73, Appendix B, Sections VI.C.1 and D.1, and is, therefore, acceptable.

Continuing Training and Qualification

The provisions of 10 CFR Part 73, Appendix B, Section VI.D.2 state, in part, that armed and unarmed individuals shall be re-qualified at least annually in accordance with the requirements of this appendix and the Commission-approved T&QP. The results of requalification must be documented by a qualified training instructor and attested by a security supervisor.

Section 3.5 of the T&QP provides discussion regarding the management of the requalification program to ensure that each individual is trained and qualified. In part, the applicant's plan provides that annual requalification may be completed up to three (3) months before or three (3) months after the scheduled date. However, the next annual training must be scheduled (12) months from the previously scheduled date rather than the date the training was actually completed.

The NRC staff has reviewed the applicant's description in T&QP Section 3.5 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the T&QP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the T&QP meets the requirements of 10 CFR Part 73, Appendix B, Section VI.D.2, and is, therefore, acceptable.

Annual Written Examination

The provisions of 10 CFR Part 73, Appendix B, Section VI.D.1(3) provide that armed individuals shall be administered an annual written exam that demonstrates the required knowledge, skills, and abilities to carry out assigned duties and responsibilities as an armed member of the security organization. The annual written exam must include those elements listed in the Commission-approved T&QP to demonstrate an acceptable understanding of assigned duties and responsibilities.

Section 3.5.1 of the T&QP provides that each individual will be tested, in part, with an annual written exam that, at a minimum, covers: the role of security personnel; use of deadly force; the requirements in 10 CFR 73.21; authority of private security personnel; power of arrest; search and seizure; offsite law enforcement response; tactics and tactical deployment and engagement.

The NRC staff has reviewed the applicant's description in T&QP Section 3.5.1 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the T&QP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the T&QP meets the requirements of 10 CFR Part 73, Appendix B, Section VI.D.1.(3), and is, therefore, acceptable.

Demonstration of Knowledge Skills and Abilities

The provisions of 10 CFR Part 73, Appendix B, Sections VI, A.4, B.2(c)(2), B.3(a), B.4(b)(1), B.4(b)(3), B.5(a), C.2(a), C.2(b), C.3(a), C.3(b) C.3(d), D.1(a), D.1(b)(1), D.1(b)(2), D.1(b)(3), and D.1(c) state, in part, that an individual must demonstrate required knowledge, skills and abilities, to carry out assigned duties and responsibilities.

Section 3.5.2 of the T&QP provides that all knowledge, skills and abilities will be demonstrated in accordance with a systematic approach to training (SAT) program as described in RG 5.75.

The NRC staff has reviewed the applicant's description in T&QP Section 3.5.2 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the T&QP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the T&QP meets the requirements of 10 CFR Part 73, Appendix B, Sections VI.A, B, C, and D and is, therefore, acceptable.

Weapons Training and Qualification

General Firearms Training

The provisions of 10 CFR Part 73, Appendix B, Section VI.E provide that armed members of the security organization shall be trained and qualified in accordance with the requirements of this appendix and the Commission-approved T&QP. Training must be conducted by certified

firearms instructors who shall be recertified at least every three (3) years. Applicants shall conduct annual firearms familiarization, and armed members of the security organization must participate in weapons range activities on a nominal four (4) month periodicity.

Section 3.6.1 of the T&QP addresses the requirements in 10 CFR Part 73, Appendix B, Sections VI.E.1(d)(1) through (11) and includes the requirements for training in the use of deadly force and participation in weapons range activities on a nominal four (4) month periodicity.

The NRC staff has reviewed the applicant's description in T&QP Section 3.6.1 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the T&QP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the T&QP meets the requirements of 10 CFR Part 73, Appendix B, Section VI.E.1, and is, therefore, acceptable.

General Weapons Qualification

The provisions of 10 CFR Part 73, Appendix B, Section VI.F.1 Weapons Qualification and Requalification Program require that qualification firing must be accomplished in accordance with Commission requirements and the Commission-approved T&QP for assigned weapons. The results of weapons qualification and requalification must be documented and retained as a record.

Section 3.6.2 of the T&QP provides that all armed personnel are qualified and re-qualified with assigned weapons. All weapons qualification and re-qualification will be documented and retained as a record.

The NRC staff has reviewed the applicant's description in T&QP Section 3.6.2 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the T&QP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the T&QP meets the requirements of 10 CFR Part 73, Appendix B, Section VI.F.1, and is, therefore, acceptable.

Tactical Weapons Qualification

The provisions of 10 CFR Part 73, Appendix B, Section VI.F.2 require that the applicant conduct tactical weapons qualification. The applicant T&QP must describe the firearms used, the firearms qualification program, and other tactical training required to implement the Commission-approved security plans, applicant protective strategy, and implementing procedures. Applicant developed tactical qualification and requalification courses must describe the performance criteria needed to include the site specific conditions (such as lighting, elevation, fields-of-fire) under which assigned personnel shall be required to carry out their assigned duties.

Section 3.6.3 of the T&QP provides that a tactical qualification course of fire is used to assess armed security force personnel in tactical situations to ensure they are able to demonstrate required tactical knowledge, skills and abilities remain proficient.

The NRC staff has reviewed the applicant's description in T&QP Section 3.6.3 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the T&QP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the T&QP meets the requirements of 10 CFR Part 73, Appendix B, Section VI.F.3 and is, therefore, acceptable.

Firearms Qualification Courses

The provisions of 10 CFR Part 73, Appendix B, Section VI.F.3 state, in part, that the applicant shall conduct the following qualification courses for each weapon used: (a) an annual daylight fire qualification course; and (b) an annual night fire qualification course.

Courses of Fire

The provisions of 10 CFR Part 73, Appendix B, Section VI.F.4 describe required courses of fire.

Section 3.6.4 of the T&QP provides a description of the firearms qualification courses used to ensure armed members of the security organization are properly trained and qualified. Courses of fire are used individually for handguns, shotguns, and semiautomatic rifles, and enhanced weapons.

The NRC staff has reviewed the applicant's description in T&QP Section 3.6.4 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the T&QP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the T&QP meets the requirements of 10 CFR Part 73, Appendix B, Section VI.F.3, and 10 CFR Part 73, Appendix B, Section VI.F.4, and is, therefore, acceptable.

Firearms Requalification

The provisions of 10 CFR Part 73, Appendix B, Section VI.F.5 provide that armed members of the security organization shall be re-qualified for each assigned weapon at least annually in accordance with Commission requirements and the Commission-approved T&QP, and the results documented and retained as a record. Firearms requalification must be conducted using the courses of fire outlined in 10 CFR Part 73, Appendix B, Sections VI.F.2, VI.F.3, and VI.F.4.

Section 3.6.5 of the T&QP describes that armed members of the security organization re-qualify at least annually with each weapon assigned, using the courses of fire provided in the T&QP.

The NRC staff has reviewed the applicant's description in T&QP Section 3.6.5 for the implementation of the site-specific physical protection program in accordance with Commission

regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the T&QP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the T&QP meets the requirements of 10 CFR Part 73, Appendix B, Section VI.F.5, and is, therefore, acceptable.

Weapons, Personal Equipment and Maintenance

The provisions of 10 CFR Part 73, Appendix B, Section VI.G provide the requirements for the maintenance of weapons and personal equipment. These requirements provide that the applicant shall provide armed personnel with weapons that are capable of performing the function stated in the Commission-approved security plans, applicant protective strategy, and implementing procedures. In addition, the applicant shall ensure that each individual is equipped or has ready access to all personal equipment or devices required for the effective implementation of the Commission-approved security plans, applicant protective strategy, and implementing procedures.

Section 3.7 of the T&QP describes that personnel are provided with weapons and personal equipment necessary to meet the plans and the protective strategy. The equipment provided is described in Section 9.0 of the PSP, and maintenance is performed as described in Section 20.0 of the PSP.

The NRC staff has reviewed the applicant's description in T&QP Section 3.7 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the T&QP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the T&QP meets the requirements of 10 CFR Part 73, Appendix B, Section VI.G, and is, therefore, acceptable. The staff's review of Sections 9.0 and 20.0 of the PSP is in Section 13.6.4.1.9 and 13.6.4.1.20 of this SER.

Documentation

The provisions of 10 CFR Part 73, Appendix B, Section VI.H require that the applicant shall retain all reports, records, or other documentation required by this appendix in accordance with the requirements of 10 CFR 73.55(r). The applicant shall retain each individual's initial qualification record for three (3) years after termination of the individual's employment and shall retain each re-qualification record for three (3) years after it is superseded. The applicant shall document data and test results from each individual's suitability, physical, and psychological qualification and shall retain this documentation as a record for three (3) years from the date of obtaining and recording these results.

Section 3.8 of the T&QP provides that records are retained in accordance with Section 22 of the PSP.

The NRC staff has reviewed the applicant's description in T&QP Section 3.8 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the T&QP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds

that the description provided in the T&QP meets the requirements of 10 CFR Part 73, Appendix B, Section VI.H and is, therefore, acceptable.

The following portion of this technical evaluation section is reproduced from Section 13.6.4.2 of the VEGP SER:

*13.6.4.2.4 Performance Evaluation Program*

*10 CFR Part 73, Appendix B, Section VI.C.3, Performance Evaluation Program*

*(a) Applicants shall develop, implement and maintain a performance evaluation program that is documented in procedures, which describes how the applicant will demonstrate and assess the effectiveness of their onsite physical protection program and protective strategy, including the capability of the armed response team to carry out their assigned duties and responsibilities during safeguards contingency events. The performance evaluation program and procedures shall be referenced in the applicant's T&QP.*

*(b) The performance evaluation program shall include procedures for the conduct of tactical response drills and force-on-force exercises designed to demonstrate and assess the effectiveness of the applicant's physical protection program, protective strategy and contingency event response by all individuals with responsibilities for implementing the SCP. The performance evaluation program must be designed to ensure, in part, that each member of each shift who is assigned duties and responsibilities required to implement the SCP and applicant protective strategy participates in at least one tactical response drill on a quarterly basis and one force-on-force exercise on an annual basis.*

*Section 4 of the T&QP details the performance evaluation program consistent with the requirements of 10 CFR Part 73, Appendix B, Sections VI.C.3(a) through (m). Additional details of the performance evaluation program are described in the facility procedures.*

*The NRC staff has reviewed the applicant's description in T&QP Section 4 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the T&QP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the T&QP meets the requirements of 10 CFR Part 73, Appendix B, Section VI.C.3 and is, therefore, acceptable.*

*13.6.4.2.5 Definitions*

*The provisions of 10 CFR Part 73, Appendix B, Section VI.J state, in part, that terms defined in 10 CFR Part 50, 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material," and 10 CFR Part 73 have the same meaning when used in this appendix. Definitions are found in the PSP, Appendix A, "Glossary*

*of Terms and Acronyms."* [On the basis of its review, the NRC staff finds that the definitions sections of the PSP meet the requirements of 10 CFR 73.2, and are, therefore, acceptable.]

*Included in this section of the T&QP is the Critical Task Matrix, which is considered SGI and has not been included in this SER.*

*The NRC staff has reviewed the applicant's description in T&QP of the Critical Task Matrix tasks for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the T&QP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the T&QP meets the requirements of 10 CFR Part 73, Appendix B, and are, therefore, acceptable.*

*13.6.4.2.6 Conclusion on the Training and Qualification Plan*

*On the basis of the NRC staff's review described in Sections 13.6.4.2.1 through 13.6.4.2.5 of this SER, the T&QP meets the requirements of 10 CFR Part 73, Appendix B. The target sets, Target Set Analysis and Site Protective Strategy are in the facility implementing procedures, which were not subject to NRC staff review as part of this COL application and are, therefore, subject to future NRC inspection in accordance with 10 CFR 73.55(c)(7)(iv) and 10 CFR Part 73, Appendix C, Section II.B.5(iii). The NRC staff concludes that complete and procedurally correct implementation will provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.*

*13.6.4.3 Appendix C Safeguards Contingency Plan*

*13.6.4.3.1 Background Information*

*This category of information identifies the perceived dangers and incidents that the plan addresses and a general description of how the response is organized.*

*Purpose of the Safeguards Contingency Plan*

*The provisions of 10 CFR Part 73, Appendix C, Section II.B.1.b state that the applicant should discuss general goals, objectives and operational concepts underlying the implementation of the SCP.*

*Section 1.1 of the SCP describes the purpose and goals of the SCP, including guidance to security and management for contingency events.*

*Scope of the Safeguards Contingency Plan*

*The provisions of 10 CFR Part 73, Appendix C, Section II.B.1.c delineate the types of incidents that should be covered by the applicant in the SCP, how the onsite response effort is organized and coordinated to effectively respond to a safeguards contingency event and how the onsite response for safeguards contingency events has been integrated into other site emergency response procedures.*

*Section 1.2 of the SCP details the scope of the SCP to analyze and define decisions and actions of security force personnel, as well as facility operations personnel, for achieving and maintaining safe shutdown.*

*Perceived Danger*

*The provisions of 10 CFR Part 73, Appendix C, Section II.B.1(a) require that, consistent with the DBT specified in 10 CFR 73.1(a)(1), the applicant shall identify and describe the perceived dangers, threats, and incidents against which the SCP is designed to protect.*

*Section 1.3 of the SCP outlines the threats used to design the physical protection systems.*

*The applicant adequately addresses perceived danger, provides a purpose of the plan, and describes the scope of the plan.*

*Definitions*

*Section 1.4 of the SCP describes that a list of terms and their definitions used in describing operational and technical aspects of the approved SCP as required by 10 CFR Part 73, Appendix C, Section II.B.1.d is found in Appendix A of the PSP.*

*The NRC staff has reviewed the applicant's description in SCP Sections 1, 1.1, 1.2, 1.3, and 1.4 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the SCP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the SCP meets the requirements of 10 CFR Part 73, Appendix C, Section II.D.3 and are, therefore, acceptable.*

*13.6.4.3.2 Generic Planning Base*

*As required in 10 CFR Part 73, Appendix C, Section II.B.2, this section of the plan defines the criteria for initiation and termination of responses to security events, to include the specific decisions, actions, and supporting information needed to respond to each type of incident covered by the approved SCP.*

*Situations Not Covered by the Contingency Plan*

*Section 2.1 of the SCP details the general types of conditions that are not covered in the plan.*

*Situations Covered by the Contingency Plan*

*The provisions of 10 CFR Part 73, Appendix C, Section II.B.2.a require, in part, that the plan identify those events that will be used for signaling the beginning or aggravation of a safeguards contingency according to how they are perceived initially by the applicant's personnel. Applicants shall ensure detection of unauthorized activities and shall respond to all alarms or other indications signaling a security event, such as penetration of a PA, vital area, or unauthorized barrier penetration (vehicle or personnel); tampering, bomb threats, or other threat warnings—either verbal, such as telephoned threats, or implied, such as escalating civil disturbances.*

*The provisions of 10 CFR Part 73, Appendix C, Section II.B.2.b require, in part, that the plan define the specific objective to be accomplished relative to each identified safeguards contingency event. The objective may be to obtain a level of awareness about the nature and severity of the safeguards contingency to prepare for further responses; to establish a level of response preparedness; or to successfully nullify or reduce any adverse safeguards consequences arising from the contingency.*

*The provisions of 10 CFR Part 73, Appendix C, Section II.B.2.c require, in part, that the applicant identify the data, criteria, procedures, mechanisms and logistical support necessary to achieve the objectives identified.*

*Section 2.2 of the SCP describes in detail the specific situations covered by the SCP, including objectives and information required for each.*

*The NRC staff has reviewed the applicant's description in SCP Sections 2, 2.1 and 2.2 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the SCP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the SCP meets the requirements of 10 CFR Part 73, Appendix C Section II.B.2 and are, therefore, acceptable.*

*13.6.4.3.3* Responsibility Matrix

The provisions of 10 CFR Part 73, Appendix C, Section II.B.4 state that this category of information consists of the detailed identification of responsibilities and specific actions to be taken by the applicant's organizations and/or personnel in response to safeguards contingency events. To achieve this result the applicant must address the following.

The provisions of 10 CFR Part 73, Appendix C, Section II.B.4.a require, in part, that the applicant develop site procedures that consist of matrixes detailing the organization and/or personnel responsible for decisions and actions associated with specific responses to safeguards contingency events. The responsibility matrix and procedures must be referenced in the applicant's SCP.

The provisions of 10 CFR Part 73, Appendix C, Section II.B.4.b require, in part, that the responsibility matrix procedures shall be based on the events outlined in the applicant's generic planning base and include specific objectives to be accomplished, description of responsibilities for decisions and actions for each event, and overall description of response actions each responding entity.

The provisions of 10 CFR Part 73, Appendix C, Section II.B.4.c require, in part, that responsibilities are to be assigned in a manner that precludes conflict of duties and responsibilities that would prevent the execution of the SCP and emergency response plans.

The provisions of 10 CFR Part 73, Appendix C, Section II.B.4.d require, in part, that the applicant ensure that predetermined actions can be completed under the postulated conditions.

Section 3 of the SCP includes the responsibility matrix. The responsibility matrix integrates the response capabilities of the security organization (described in Section 4 of the SCP) with the background information relating to decision/actions and organizational structure (described in Section 1 of the SCP). The responsibility matrix provides an overall description of the response actions and their interrelationships. Responsibilities and actions have been predetermined to the maximum extent possible and assigned to specific entities to preclude conflicts that would interfere with or prevent the implementation of the SCP or the ability to protect against the DBT of radiological sabotage.

The NRC staff has reviewed the applicant's description in SCP Section 3 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the SCP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the SCP meets the requirements of 10 CFR Part 73, Appendix C, Section II.B.4 and is, therefore, acceptable.

13.6.4.3.4 Licensee Planning Base

The provisions of 10 CFR Part 73, Appendix C, Section II.B.3 require, in part, that the applicant planning base include factors affecting the SCP specific for each facility.

Licensee Organization

The provisions of 10 CFR Part 73, Appendix C, Section II.B.3.a require in part, that the SCP describe the organization's chain of command and delegation of authority during safeguards contingency events, to include a general description of how command and control functions will be coordinated and maintained.

Duties/Communication Protocols

Section 4.1.1 of the SCP details the duties and communications protocols of each member of the security organization responsible for implementing any portion of the applicant's protective strategy.

Security Chain of Command/Delegation of Authority

Section 4.1.2 of the SCP details the chain of command and delegation of authority during normal operations is discussed in the PSP. The chain of command and delegation of authority during contingency events is also described in the responsibility matrix portions of the SCP. The chain of command and delegation of authority during normal operations is discussed in the PSP.

Physical Layout

The provisions of 10 CFR Part 73, Appendix C, Section II.B.3(b) require, in part, that the SCP include a site map depicting the physical structures located on the site, including onsite independent spent fuel storage installations, and a description of the structures depicted on the map. Plans must also include a description and map of the site in relation to nearby towns, transportation routes (e.g., rail, water, and roads), pipelines, airports, hazardous material facilities, and pertinent environmental features that may have an effect upon coordination of response activities. Descriptions and maps must indicate main and alternate entry routes for law enforcement or other offsite response and support agencies and the location for marshaling and coordinating response activities.

Section 4.2 of the SCP references Section 1.1 of the PSP for layouts of the OCA, PA, vital areas, site maps, and descriptions of site features.

Safeguards Systems

The provisions of 10 CFR Part 73, Appendix C, Section II.B.3.c require, in part, that the SCP include a description of the physical security systems that support and influence how the applicant will respond to an event in accordance with the DBT described in 10 CFR 73.1(a). The description must begin with onsite physical protection measures implemented at the outermost perimeter, and must move inward through those measures implemented to protect target set equipment.

Section 4.3 of the PSP describes that safeguards systems are described in PSP Sections 9, 11, 12, 13, 15 and 16, and in facility implementing procedures/documents. Section 8 of the SCP describes how physical security systems will be used to respond to a threat at the site.

Law Enforcement Assistance

The provisions of 10 CFR Part 73, Appendix C, Section II.B.3.d require in part, that the applicant provide a listing of available law enforcement agencies and a general description of their

response capabilities and their criteria for response and a discussion of working agreements or arrangements for communicating with these agencies.

Section 4.4 of the SCP details the role of LLEA in the site protective strategy. Additional details regarding LLEA are included in Section 8 of the PSP and Section 5.6 of the SCP.

Policy Constraints and Assumptions

The provisions of 10 CFR Part 73, Appendix C, Section II.B.3.e require in part, that the SCP include a discussion of State laws, local ordinances, and company policies and practices that govern applicant response to incidents and must include, but is not limited to, the following: 1) use of deadly force; 2) recall of off-duty employees; 3) site jurisdictional boundaries; and 4) use of enhanced weapons, if applicable.

Section 4.5 of the SCP details the site security policies, including the use of deadly force and authority to request offsite assistance.

Administrative and Logistical Considerations

The provisions of 10 CFR Part 73, Appendix C, Section II.B.3.f require in part, that the applicant provide descriptions of applicant practices, which influence how the security organization responds to a safeguards contingency event to include, but is not limited to, a description of the procedures that will be used for ensuring that equipment needed to facilitate response will be readily accessible, in good working order, and in sufficient supply.

Section 4.6 of the SCP outlines administrative duties of the Security Manager, Security Shift Team Leader, facility procedures and administrative forms.

The NRC staff has reviewed the applicant's description in SCP Sections 4, 4.1, 4.1.1, 4.1.2, and 4.2 through 4.6 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the SCP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the SCP meets the requirements of 10 CFR Part 73, Appendix C, Section II.B.3 and is, therefore, acceptable.

13.6.4.3.5 Response Capabilities

This section outlines the response by the applicant to threats to the facility. The applicant details how they protect against the DBT with onsite and offsite organizations, consistent with the regulation of 10 CFR 50.54(p)(1) and (hh), 10 CFR 73.55(k), 10 CFR Part 73, Appendix B, Section VI and 10 CFR Part 73, Appendix C, Section II.B.3. In addition, 10 CFR Part 73, Appendix C, "Introduction," states, in part, it is important to note that a applicant's SCP is intended to be complementary to any emergency plans developed pursuant to Appendix E to 10 CFR Part 50 and 10 CFR 52.17.

Response to Threats

Section 5.1 of the SCP describes how the protective strategy is designed to defend the facility against all aspects of the DBT. Each organization has defined roles and responsibilities.

Armed Response Team

Section 5.2 of the SCP notes individuals from the Responsibility Matrix and their role in the site protective strategy. This section also notes the minimum number of individuals and their contingency equipment for implementation of the protective strategy. The applicant described the armed response team consistent with 10 CFR 73.55(k)(4), (5), (6), and (7), 10 CFR Part 73, Appendix B, Section VI, and 10 CFR Part 73, Appendix C, Section II.B.3.

Supplemental Security Officer

Section 5.3 of the SCP details the role of supplemental security officers in the site protective strategy. The applicant described the use of supplemental security officers, consistent with the requirements in 10 CFR 73.55(k)(4).

Facility Operations Response

Section 5.4 of the SCP details the role of operations personnel in the site protective strategy, including responsibilities, strategies, and conditions for operator actions as discussed in 10 CFR 50.54(hh).

Emergency Plan Response

Section 5.5 of the SCP notes the integration of the Emergency Plan with the site's protective strategy, and gives some examples of how the Emergency Plan can influence the protective strategy as discussed in 10 CFR 73.55(b)(11).

Local Law Enforcement Agencies (LLEA)

Section 5.6 of the SCP meets the requirements of 10 CFR 73.55(k)(9) and 10 CFR Part 73, Appendix C, Section II.B.3.d and lists the LLEAs that will respond to the site as a part of the protective strategy. Details on the response of the LLEA are located in Section 8 of the PSP.

State Response Agencies

Section 5.7 of the SCP meets the requirements of 10 CFR 73.55(k)(9) and 10 CFR Part 73, Appendix C, Section II.B.3.d and lists the State response agencies that will respond to the site as a part of the protective strategy.

Federal Response Agencies

Section 5.8 of the SCP meets the requirements of 10 CFR 73.55(k)(9) and 10 CFR Part 73, Appendix C, Section II.B.3.d and lists the Federal response agencies that will respond to the site as a part of the protective strategy.

Response to ISFSI Events

VCSNS Units 2 and 3 do not have an ISFSI, so this section does not apply.

The NRC staff has reviewed the applicant's description in SCP Sections 5.0 through 5.9 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the SCP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the SCP meets the requirements of 10 CFR 50.54(p)(1) and (hh), 10 CFR 73.55(k), 10 CFR Part 73, Appendix B, Section VI and 10 CFR Part 73, Appendix C, Section II.B.3 and is, therefore, acceptable. In addition, Appendix C, "Introduction" states, in part, that it is important to note that an applicant's SCP is intended to be complementary to any emergency plans developed pursuant to Appendix E to 10 CFR Part 50 and 10 CFR 52.17.

The following portion of this technical evaluation section is reproduced from Section 13.6.4.3 of the VEGP SER:

> *13.6.4.3.6 Defense-In-Depth*
>
> *Section 6 of the SCP lists site physical security characteristics, programs, and the strategy elements that illustrate the defense-in-depth nature of the site protective strategy as required in 10 CFR 73.55(b)(3).*
>
> *The NRC staff has reviewed the applicant's description in SCP Section 6 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the SCP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the SCP meets the requirements of 10 CFR 73.55(b)(3) and is, therefore, acceptable.*
>
> *13.6.4.3.7 Primary Security Functions*
>
> *Section 7 of the SCP details the primary security functions of the site, and their roles in the site protective strategy. It also notes the development of target sets, and their function in the development of the site's protective strategy.*
>
> *The NRC staff has reviewed the applicant's description in SCP Section 7 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because*

*the applicant's description in the SCP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the SCP meets the requirements of 10 CFR 10 CFR 73.55(b) and is, therefore, acceptable.*

13.6.4.3.8 Protective Strategy

The provisions of 10 CFR Part 73, Appendix C, Section II.B.3.c(v) require that applicants develop, implement and maintain a written protective strategy that shall: 1) be designed to meet the performance objectives of 10 CFR 73.55(a) through (k); 2) identify predetermined actions, areas of responsibilities, and timelines for the deployment of armed personnel; 3) include measures that limit the exposure of security personnel to possible attack; 4) include a description of the physical security systems and measures that provide defense-in-depth; 5) describe the specific structure and responsibilities of the armed response organization; and 6) provide a command and control structure.

Section 8 of the SCP describes the site protective strategy.

The NRC staff has reviewed the applicant's description in SCP Section 8 for the implementation of the site-specific physical protection program in accordance with Commission regulations and NUREG-0800 acceptance criteria. Because the applicant's description in the SCP is consistent with the acceptance criteria in NUREG-0800, Section 13.6.1, the staff finds that the description provided in the SCP meets the requirements of 10 CFR Part 73, Appendix C, Section II.B.3.c(v) and is, therefore, acceptable.

The following portion of this technical evaluation section is reproduced from Section 13.6.4.3 of the VEGP SER:

*13.6.4.3.9 Conclusions on the Safeguards Contingency Plan*

*On the basis of the NRC staff's review described in Sections 13.6.4.3.1 through 13.6.4.3.8 of this SER, the SCP meets the requirements of 10 CFR Part 73, Appendix C, in accordance with the DBT of radiological sabotage as stated in 10 CFR 73.1. The target sets, Target Set Analysis and Site Protective Strategy are in the facility implementing procedures, which were not subject to NRC staff review as part of this COL application and are, therefore, subject to future NRC inspection in accordance with 10 CFR 73.55(c)(7)(iv) and 10 CFR Part 73, Appendix C, Section II.B.5(iii). The NRC staff concludes that complete and procedurally correct implementation of the SCP will provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.*

**13.6.5 Post Combined License Activities**

For the reasons discussed in the technical evaluation section above, the staff finds the following license condition proposed by the applicant acceptable:

- License Condition (13-5) - The licensee shall submit to the Director of NRO, a schedule, no later than 12 months after issuance of the COL, that supports planning for and conduct of NRC inspection of the physical security programs. The schedule shall be updated every 6 months until 12 months before scheduled fuel load, and every month thereafter until either the physical security program has been fully implemented or the plant has been placed in commercial service, whichever comes first.

### 13.6.6 Conclusion

The NRC staff reviewed the application and checked the referenced DCD. The NRC staff's review confirmed that the applicant addressed the required information relating to physical security, and there is no outstanding information expected to be addressed in the VCSNS COL FSAR related to this section. The results of the NRC staff's technical evaluation of the information incorporated by reference in the VCSNS COL application are documented in NUREG-1793 and its supplements.

The staff concludes that, pending closure of **Confirmatory Items 13.6-1 and 13.6-2**, the relevant information presented in the VCSNS COL FSAR is acceptable based on the applicable regulations specified in Section 13.6.4 of this SER. The staff based its conclusion on the following:

- STD COL 13.6-1, as related to the physical protection program, is acceptable based on the following discussion. The NRC staff's review of the VCSNS Units 2 and 3 PSP, T&QP, and SCP has focused on ensuring the necessary programmatic elements are included in these plans to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.

  The NRC staff has determined that these plans include the necessary programmatic elements that, when effectively implemented, will provide the required high assurance. The burden to effectively implement these plans remains with the applicant. Effective implementation is dependent on the procedures and practices the applicant develops to satisfy the programmatic elements of its PSP, T&QP, and SCP. The NRC staff has not reviewed the site-specific target set analysis, site protective strategy and the facility implementing procedures. The target set analysis, site protective strategy and the facility implementing procedures are subject to future NRC inspections and review. As required by Section 3 of the applicant's PSP, a performance evaluation program will be implemented that periodically tests and evaluates the effectiveness of the overall protective strategy. This program requires that deficiencies be corrected. In addition, NRC inspectors will conduct periodic force-on-force exercises that will test the effectiveness of the applicant's protective strategy. Based on the results of the applicant's own testing and evaluation, the NRC's baseline inspections and force-on-force exercises, enhancements to the applicant's PSP, T&QP, and SCP may be required to ensure the overall protective strategy can be effectively implemented. As such, staff approval of the applicant's PSP, T&QP, and SCP is limited to the programmatic elements necessary to provide the required high assurance as stated

above. Should deficiencies be identified with the programmatic elements of these plans as a result of the periodic applicant or NRC conducted drills or exercises that test the effectiveness of the overall protective strategy, the plans shall be corrected to address these deficiencies in a timely manner and to notify the NRC of these plan changes in accordance with the requirements of 10 CFR 50.54(p) or 10 CFR 50.90.

The COL applicant's security plan information is withheld from public disclosure in accordance with the provisions of 10 CFR 73.21.

## 13.6.A Site-Specific ITAAC for Physical Security

13.6.A.1 Introduction

Part 10, "Proposed License Conditions and ITAAC," Appendix B, "Inspections, Tests, Analysis, and Acceptance Criteria" of the VCSNS COL application describes the license conditions for the plant's physical protection systems or features to provide physical protection of the site specific protective strategy and elements of a site security program. The COL application incorporates by reference the Tier 1 Section 2.6.9 of the AP1000 DCD, including plant layout and configurations of barriers, and lists ITAAC related to the site-specific design for achieving detection, assessment, communications, delay, and response for physical protection against potential acts of radiological sabotage and theft of special nuclear material.

The design bases or supporting security analyses and assumptions related to the design descriptions of security-related features incorporated by reference from the AP1000 DCD are in Technical Report #94, APP-GW-GLR-066. Descriptions of site-specific security structures, programs and contingency measures are in the VCSNS PSP, which includes the site PSP, T&QP and the SCP.

13.6.A.2 Summary of Application

Section 14.3 of the VCSNS COL FSAR, Revision 2, incorporates by reference Section 14.3 of the AP1000 DCD, Revision 17. Part 10, Revision 2 of the VCSNS COL application incorporates by reference DCD Tier 1 Section 2.6.9, which includes the physical security ITAAC that are in the scope of the AP1000 standard design. Site-specific physical security-ITAAC (PS-ITAAC) that are outside the scope of AP1000 DCD Tier 1 Section 2.6.9 are provided in Table 2.6.9-2 of Appendix B to Part 10 of the VCSNS COL application.

In addition, in VCSNS COL FSAR Section 14.3, the applicant provided the following:

*Supplemental Information*

- STD SUP 14.3-1

The applicant provided supplemental information related to physical security in STD SUP 14.3-1 in VCSNS COL FSAR Section 14.3.2.3.2.

*License Condition*

- Part 10, License Condition 1

The applicant provided a license condition in Part 10 of the VCSNS COL application, Revision 2, which will incorporate the ITAAC identified in the tables in Appendix B. The staff evaluates this license condition in Chapter 1 of this SER.

13.6.A.3 Regulatory Basis

The regulatory basis of the information incorporated by reference is addressed in NUREG-1793 and its supplements.

In addition, the acceptance criteria associated with the relevant requirements of the Commission regulations are given in 10 CFR Part 73. The regulation includes specific security and performance requirements that, when adequately implemented, are designed to protect nuclear power reactors against acts of radiological sabotage, prevent the theft or diversion of special nuclear material, and protect safeguards information against unauthorized release.

The provisions of 10 CFR 52.80, Subpart A require that information submitted for a COL include the proposed ITAAC that the licensee shall perform, and the acceptance criteria that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, analyses, and acceptance criteria are met, the facility has been constructed and will operate in conformity with the COL, the provisions of the Atomic Energy Act, and the NRC's regulations.

The VCSNS Units 2 and 3 design descriptions, commitments, and acceptance criteria for the security features, including the plant's layout and determination of vital equipment and areas, for a certified design are based on physical protection systems or hardware provided for meeting requirements of the following Commission regulations:

- 10 CFR Part 50, "Domestic licensing of production and utilization facilities"
- 10 CFR Part 52, "Licenses, certifications, and approvals for nuclear power plants"
- 10 CFR 73.1(a)(1), "Radiological sabotage"
- 10 CFR 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage," and Appendices B, C, G and H
- 10 CFR Part 74, "Material control and accounting of special nuclear material"
- 10 CFR 100.21(f), "Non-seismic siting criteria"

Regulatory requirements and acceptance criteria related to physical protection systems or hardware are identified in Section 14.3.12 of NUREG-0800.

Regulatory guidance documents that are applicable to this evaluation are:

- RG 1.91, “Evaluations of Explosions Postulated to Occur at Transportation Routes Near Nuclear Power Plants,” Revision 1
- RG 1.206, “Combined License Applications for Nuclear Power Plants”
- RG 4.7, “General Site Suitability Criteria for Nuclear Power Stations,” Revision 2
- RG 5.12, “General Use of Locks in the Protection and Control of Facilities and Special Nuclear Materials”
- RG 5.62, “Reporting of Safeguards Events,” Revision 1
- RG 5.65, “Vital Area Access Controls, Protection of Physical Security Equipment and Key and Lock Controls”
- RG 5.66, “Access Authorization Program for Nuclear Power Plants”
- RG 5.7, “Entry/Exit Control for Protected Areas, Vital Areas, and Material Access Areas,” Revision 1
- RG 5.44, “Perimeter Intrusion Alarm Systems,” Revision 3
- Information Notice 86-83, “Underground Pathways into Protected Areas, Vital Areas, and Controlled Access Areas,” September 19, 1986.
- Regulatory Information Summary (RIS) 2005-04, “Guidance on the Protection of Unattended Openings that Intersect a Security Boundary or Area,” April 14, 2005. (Exempt from public disclosure in accordance with 10 CFR 2.390)

The COL applicant is required to describe commitments for establishing and maintaining a physical protection system (engineered and administrative controls), organization, programs, and procedures for implementing a site-specific strategy that, if adequately implemented, provide high assurance for protection of the plant against the DBT. The site-specific physical protection system described must be reliable and available and implement the concept of defense-in-depth protection in order to provide a high assurance of protection. The security operational programs and the physical protection system are required to meet the specific performance requirements of 10 CFR Part 26, 10 CFR 73.54, 10 CFR 73.55,10 CFR 73.56, 10 CFR 73.57, and 10 CFR 73.58. Physical protection hardware within the scope of the AP1000 design is addressed in the AP1000 DCD.

13.6.A.4 Technical Evaluation

The NRC staff reviewed Section 14.3 of the VCSNS COL FSAR and checked the referenced DCD to ensure that the combination of the DCD and the COL application represents the complete scope of information relating to this review topic.[1] The NRC staff’s review confirmed that the information in the application and incorporated by reference addresses the required

information relating to ITAAC for physical security. The results of the NRC staff's evaluation of the information incorporated by reference in the VCSNS COL application are documented in NUREG-1793 and its supplements.

Section 1.2.3 of this SER provides a discussion of the strategy used by the NRC to perform one technical review for each standard issue outside the scope of the DC and use this review in evaluating subsequent COL applications. To ensure that the staff's findings on standard content that were documented in the SER for the reference COL application (VEGP Units 3 and 4) were equally applicable to the VCSNS Units 2 and 3 COL application, the staff undertook the following reviews:

- The staff compared the VEGP COL FSAR, Revision 2 to the VCSNS COL FSAR. In performing this comparison, the staff considered changes made to the VCSNS COL FSAR (and other parts of the COL application, as applicable) resulting from RAIs.

- The staff confirmed that all responses to RAIs identified in the corresponding standard content evaluation were endorsed.

- The staff verified that the site-specific differences were not relevant.

The staff has completed its review and found the evaluation performed for the standard content to be directly applicable to the VCSNS COL application. This standard content material is identified in this SER by use of italicized, double-indented formatting. The staff confirmed that the July 1, 2010, VCSNS letter contained the same technical information provided in the June 11, 2010, VEGP letter discussed in the standard content material below.

The following portion of this technical evaluation section is reproduced from Section 13.6.A.4 of the VEGP SER:

*Supplemental Information*

- *STD SUP 14.3-1*

*STD SUP 14.3-1 adds the following after DCD Section 14.3.2.2 as new Section 14.3.2.3.2:*

> *Generic PS-ITAAC have been developed in a coordinated effort between the NRC and the Nuclear Energy Institute (NEI) as outlined in Appendix C.II.I-C of Regulatory Guide 1.206. These generic ITAAC have been tailored to the AP1000 design and site-specific security requirements.*

*In Part 10, Appendix B of the VEGP Units 3 and 4 COL application, SNC describes the ITAAC for the plant's physical protection systems or features to provide physical protection of the site-specific protective strategy and elements of a site security program. The COL application incorporates by reference Tier 1 Section 2.6.9 of the AP1000 DCD, including plant layout and configurations of*

*barriers, and listed ITAAC related to the site-specific design for achieving detection, assessment, communications, delay, and response for physical protection against potential acts of radiological sabotage and theft of special nuclear material. DCD Tier 1 Section 2.6.9 includes the physical security ITAAC that are in the scope of the AP1000 standard design. Site-specific physical security ITAAC that are outside the scope of AP1000 DCD Tier 1 Section 2.6.9 are provided in Table 2.6.9-2 of Appendix B to Part 10 of the VEGP COL application.*

*The NRC staff's evaluation of the PS-ITAAC (STD SUP 14.2-1) is documented in the Sections 13.6.A.4.1 through 13.6.A.4.3 of this SER.*

*13.6.A.4.1 Detection and Assessment Hardware*

*The applicant submitted the following ITAAC for detection and assessment hardware in their letter dated June 11, 2010, "Response to Request for Additional Information Letter No. 047, Supplement 2, Physical Security Inspections, Tests, Analyses, and Acceptance Criteria," This letter was used to complete the evaluation below.*

1. *The external walls, doors, ceiling, and floors in the location within which the last access control function for access to the protected area is performed are bullet resistant to at least Underwriters Laboratory Ballistic Standard 752, Level 4. (Item 6 in Appendix A to Section 14.3.12 of NUREG-0800.)*

2. *Physical barriers for the protected area perimeter are not part of vital area barriers. (Item 2.a in Appendix A to Section 14.3.12 of NUREG-0800.)*

3. 
   a) *Isolation zones exist in outdoor areas adjacent to the physical barrier at the perimeter of the protected area that allows 20 feet of observation on either side of the barrier. (Item 3.a in Appendix A to Section 14.3.12 of NUREG-0800.)*

   b) *Where permanent buildings do not allow a 20-foot observation distance on the inside of the protected area, the building walls are immediately adjacent to, or an integral part of, the protected area barrier. (Item 3.c in Appendix A to Section 14.3.12 of NUREG-0800.) The isolation zones are monitored with intrusion detection equipment that provides the capability to detect and assess unauthorized persons. (Item 3.b in Appendix A to Section 14.3.12 of NUREG-0800.)*

4. *The intrusion detection and assessment equipment at the protected area perimeter:*

*a) Detects penetration or attempted penetration of the protected area barrier and concurrently alarms in both the Central Alarm Station and Secondary Alarm Station. (Item 4.a in Appendix A to Section 14.3.12 of NUREG-0800.)*

*b) The intrusion detection and assessment equipment at the protected area perimeter remains operable from an uninterruptible power supply in the event of the loss of normal power. (Item 4.c in Appendix A to Section 14.3.12 of NUREG-0800.)*

*6. An access control system with numbered picture badges is installed for use by individuals who are authorized access to protected areas without escort. (Item 9 in Appendix A to Section 14.3.12 of NUREG-0800.)*

*8.*

*a) Penetrations through the protected area barrier are secured and monitored. (Item 2.b in Appendix A to Section 14.3.12 of NUREG-0800.)*

*b) Unattended openings (such as underground pathways) that intersect the protected area boundary or vital area boundary will be protected by a physical barrier and monitored by intrusion detection equipment or provided surveillance at a frequency sufficient to detect exploitation. (Item 2.c in Appendix A to Section 14.3.12 of NUREG-0800.)*

*On the basis of its review the NRC staff determined that the applicant has adequately revised Table 2.6.9-2 for Part 10 to the VEGP COL application PS-ITAAC items 2(a), 2(b), 2 (c), 3(a), 3(b), 3(c), 4(a), 4(c), 6(partially), and 9 identified in Appendix A to Section 14.3.12 of NUREG-0800.*

*The VEGP COL application references the AP1000 DCD, which addressed NUREG-0800, Section 14.3.12 PS-ITAAC 4(b), 5, 6(partially), 10, 11(a), 11(b), 11(c) and 14. The staff has determined that PS-ITAAC 6, described in NUREG-0800, Section 14.3.12 has been fully addressed between the VEGP submission and the AP1000 DCD.*

*In a supplemental response to RAI 14.3.12-1, the applicant stated:*

*The information contained in SRP ITAAC number 11(d) is redundant to existing ITAAC in the AP1000 Design Certification Document (DCD). AP1000 DCD security ITAAC numbers 1, 4, 5(a), 5(b), 5(c), 13(a), 13(b), 13(c), and 15(b) demonstrate that the central and secondary alarm stations are equal and redundant, by being constructed, located, protected, and equipped to the standards for the central alarm station.*

*In RAI SRP 14.3.12-NSIR-7, Revision 1, Westinghouse stated:*

*No corresponding ITAAC has been provided for SRP 14.3.12 ITAAC number 11(d). The information contained in SRP ITAAC number 11(d) is redundant to existing ITAACs. AP1000 security ITAAC numbers 1, 4, 5(a), 5(b), 5(c), 13, and 15(b) demonstrate that the central and secondary alarm stations are constructed, located, protected, and equipped to the standards for the central alarm station.*

*On the basis of its review, the NRC staff determined that the applicant has adequately shown that NUREG-0800, Section 14.3.12 detection and assessment hardware ITAAC 11(d) is addressed.*

*13.6.A.4.2 Delay or Barrier Design*

*The applicant submitted the following ITAAC for Delay or Barrier Design in their "Response to Request for Additional Information Letter No. 047, Supplement 2, Physical Security Inspections, Tests, Analyses, and Acceptance Criteria," Dated June 11 2010. This letter was used to complete the evaluation below.*

5. *Access control points are established to:*

   a) *Control personnel and vehicle access into the protected area. (Item 8.a in Appendix A to Section 14.3.12 of NUREG-0800.)*

   b) *Detect firearms, explosives, and incendiary devices at the protected area personnel access points. (Item 8.b in Appendix A to Section 14.3.12 of NUREG-0800.)*

7. *Access to vital equipment physical barriers requires passage through the protected area perimeter barrier. (Item 1.b in Appendix A to Section 14.3.12 of NUREG-0800.)*

*On the basis of its review, the NRC staff determined that the applicant has adequately addressed NUREG-0800, Section 14.3.12 delay or barrier design PS-ITAAC 1(b)(partially),8(a) and 8(b).*

*The VEGP COL application references the AP1000 DCD, which addressed NUREG-0800, Section 14.3.12 PS-ITAAC 1(a), 1(b)(partially), 7, 13(a) and 13(b). The staff has determined that PS-ITAAC 1(b) described in NUREG-0800, Section 14.3.12 has been fully addressed between the VEGP submission and the AP1000 DCD.*

*13.6.A.4.3 Systems, Hardware, or Features Facilitating Security Response and Neutralization*

*The applicant submitted the following ITAAC for Systems, Hardware, or Features Facilitating Security Response and Neutralization in their "Response to Request*

*for Additional Information Letter No. 047, Supplement 2, Physical Security Inspections, Tests, Analyses, and Acceptance Criteria," Dated June 11, 2010. This letter was used to complete the evaluation below.*

*9. Emergency exits through the protected area perimeter are alarmed and secured with locking devices to allow for emergency egress. (Item 15 in Appendix A to Section 14.3.12 of NUREG-0800.)*

*On the basis of its review, the NRC staff determined that the applicant has adequately addressed NUREG-0800, Section 14.3.12 delay or barrier design PS-ITAAC 15(partially).*

*The VEGP COL application references the AP1000 DCD, which addressed NUREG-0800, Section 14.3.12 PS-ITAAC 12, 15(partially) 16(a), 16(b) and 16(c). The staff has determined that PS-ITAAC 15 described in NUREG-0800, Section 14.3.12 has been fully addressed between the VEGP submission and the AP1000 DCD.*

13.6.A.5 Post-Combined License Activities

For the reasons discussed in the technical evaluation section above, the staff proposes to include the following ITAAC for physical security:

- The licensee shall perform and satisfy the ITAAC defined in Table 13.6A-1, "Site Specific Physical Security."

13.6.A.6 Conclusion

The NRC staff reviewed the application and checked the referenced DCD. The NRC staff's review confirmed that the applicant addressed the required information relating to PS-ITAAC, and there is no outstanding information expected to be addressed in the VCSNS COL FSAR related to this section. The results of the NRC staff's technical evaluation of the information incorporated by reference in the VCSNS COL application are documented in NUREG-1793 and its supplements.

The staff concludes that the relevant information presented in VCSNS COL FSAR and the additional information received in the letter dated June 11, 2010, is acceptable based on the applicable regulations specified in Section 13.6.A.4 of this SER. The staff based its conclusion on the following:

- STD SUP 14.3-1, as related to PS-ITAAC, is acceptable based on the following discussion. The NRC staff finds that the applicant adequately describes the physical security systems or provides and/or facilitates the implementation of the site-specific protective strategy and security programs. The applicant adequately describes the site-specific PS-ITAAC for meeting the requirements of 10 CFR 73.55 and provides the technical bases for establishing a PS-ITAAC for the protection against acts of radiological sabotage and theft of special nuclear material. The applicant includes

systems and features as stated in VCSNS COL FSAR Chapter 13 and referenced TRs. The applicant has provided adequate descriptions of objectives, prerequisites, test methods, data required, and acceptance criteria for security related ITAAC for the approval of the VCSNS COL.

**Table 13.6A-1 – Site-Specific Physical Security Inspections, Tests, Analyses and Acceptance Criteria**

| Design Commitment | Inspections, Tests, and Analyses | Acceptance Criteria |
|---|---|---|
| 1. The external walls, doors, ceiling, and floors in the location within which the last access control function for access to the protected area is performed are bullet-resistant to at least Underwriters Laboratory Ballistic Standard 752, level 4. | Type test, analysis, or a combination of type test and analysis will be performed for the external walls, doors, ceilings, and floors in the location within which the last access control function for access to the protected area is performed. | The external walls, doors, ceilings, and floors in the location within which the last access control function for access to the protected area is performed are bullet- resistant to at least Underwriters Laboratory Ballistic Standard 752, level 4. |
| 2. Physical barriers for the protected area perimeter are not part of vital area barriers. | An inspection of the protected area perimeter barrier will be performed. | Physical barriers at the perimeter of the protected area are separated from any other barrier designated as a vital area barrier. |
| 3.<br>a) Isolation zones exist in outdoor areas adjacent to the physical barrier at the perimeter of the protected area that allows 20 feet of observation on either side of the barrier. Where permanent buildings do not allow a 20-foot observation distance on the inside of the protected area, the building walls are immediately adjacent to, or an integral part of, the protected area barrier. | Inspections will be performed of the isolation zones in outdoor areas adjacent to the physical barrier at the perimeter of the protected area. | Isolation zones exist in outdoor areas adjacent to the physical barrier at the perimeter of the protected area and allow 20 feet of observation and assessment of the activities of people on either side of the barrier. Where permanent buildings do not allow a 20-foot observation and assessment distance on the inside of the protected area, the building walls are immediately adjacent to, or an integral part of, the protected area barrier and the 20-foot observation and assessment distance does not apply. |
| b) The isolation zones are monitored with intrusion detection equipment that provides the capability to detect and assess unauthorized persons. | Inspections will be performed of the intrusion detection equipment within the isolation zones. | The isolation zones are equipped with intrusion detection equipment that provides the capability to detect and assess unauthorized persons. |

**Table 13.6A-1 – Site-Specific Physical Security Inspections, Tests, Analyses and Acceptance Criteria**

| Design Commitment | Inspections, Tests, and Analyses | Acceptance Criteria |
|---|---|---|
| 4. The intrusion detection and assessment equipment at the protected area perimeter:<br><br>a) detects penetration or attempted penetration of the protected area barrier and concurrently alarms in both the central alarm station and secondary alarm station, and<br><br>b) remains operable from an uninterruptible power supply in the event of the loss of normal power. | Tests, inspections or a combination of tests and inspections of the intrusion detection and assessment equipment at the protected area perimeter and its uninterruptible power supply will be performed. | The intrusion detection and assessment equipment at the protected area perimeter:<br><br>a) detects penetration or attempted penetration of the protected area barrier and concurrently alarms in the central alarm station and secondary alarm station, and<br><br>b) remains operable from an uninterruptible power supply in the event of the loss of normal power. |
| 5. Access control points are established to:<br><br>a) control personnel and vehicle access into the protected area.<br><br>b) detect firearms, explosives, and incendiary devices at the protected area personnel access points. | Tests, inspections, or combination of tests and inspections of installed systems and equipment at the access control points to the protected area will be performed. | The access control points for the protected area:<br><br>a) are configured to control personnel and vehicle access.<br><br>b) include detection equipment that is capable of detecting firearms, incendiary devices, and explosives at the protected area personnel access points. |
| 6. An access control system with numbered picture badges is installed for use by individuals who are authorized access to protected areas and vital areas without escort. | A test of the access control system with numbered picture badges will be performed. | The access authorization system with numbered picture badges can identify and authorize protected area and vital area access only to those personnel with unescorted access authorization. |
| 7. Access to vital equipment physical barriers requires passage through the protected area perimeter barrier. | Inspection will be performed to confirm that access to vital equipment physical barriers requires passage through the protected area perimeter barrier. | Vital equipment is located within a protected area such that access to vital equipment physical barriers requires passage through the protected area perimeter barrier. |

**Table 13.6A-1 – Site-Specific Physical Security Inspections, Tests, Analyses and Acceptance Criteria**

| Design Commitment | Inspections, Tests, and Analyses | Acceptance Criteria |
|---|---|---|
| 8.<br>a) Penetrations through the protected area barrier are secured and monitored. | Inspections will be performed of penetrations through the protected area barrier. | Penetrations and openings through the protected area barrier are secured and monitored. |
| b) Unattended openings (such as underground pathways) that intersect the protected area boundary or vital area boundary will be protected by a physical barrier and monitored by intrusion detection equipment or provided surveillance at a frequency sufficient to detect exploitation. | Inspections will be performed of unattended openings that intersect the protected area boundary or vital area boundary. | Unattended openings (such as underground pathways) that intersect the protected area boundary or vital area boundary are protected by a physical barrier and monitored by intrusion detection equipment or provided surveillance at a frequency sufficient to detect exploitation. |
| 9. Emergency exits through the protected area perimeter are alarmed and secured with locking devices to allow for emergency egress. | Tests, inspections, or a combination of tests and inspections of emergency exits through the protected area perimeter will be performed. | Emergency exits through the protected area perimeter are alarmed and secured by locking devices that allow prompt egress during an emergency. |

## 13.7 Fitness for Duty

### 13.7.1 Introduction

Pursuant to 10 CFR 52.79(a)(44), COL applications must include a description of the FFD program required by 10 CFR Part 26, "Fitness for Duty Programs," and its implementation. The FFD program is designed to provide reasonable assurance that: (1) individuals are trustworthy and reliable as demonstrated by the avoidance of substance abuse; (2) individuals are not under the influence of any substance, legal or illegal, or mentally or physically impaired from any cause, which in any way adversely affects their ability to safely and competently perform their duties; (3) measures are established and implemented for the early detection of individuals who are not fit to perform their duties; (4) the construction site is free from the presence and effects of illegal drugs and alcohol; (5) the work places are free from the presence and effects of illegal drugs and alcohol; and, (6) the effects of fatigue and degraded alertness on an individual's ability to safely and competently perform his or her duties are managed commensurate with maintaining public health and safety.

### 13.7.2 Summary of Application

VCSNS COL FSAR Section 13.7 is a new section added after Section 13.6 of the AP1000 DCD. The references that are currently in AP1000 DCD Section 13.7 have been redistributed to other VCSNS COL FSAR sections. There is no information associated with the FFD program incorporated by reference from the AP1000 DCD.

In addition, in VCSNS COL FSAR Section 13.7, the applicant provided the following:

*Supplemental Information*

- STD SUP 13.7-1

The applicant provided standard supplemental information in VCSNS COL FSAR Section 13.7 describing the FFD program for both the construction phase and the operating phase of the units. The construction phase program will be consistent with NEI 06-06, "Fitness for Duty Program Guidance for New Nuclear Power Plant Construction Sites," and the construction phase program will be implemented prior to onsite construction of safety- and security-related structures, systems, and components (SSCs). The operations phase program will be consistent with 10 CFR Part 26.

*License Conditions*

- Part 10, License Condition 6

The applicant proposed a license condition to provide a schedule to support the NRC's inspection of operational programs included in the VCSNS COL FSAR Table 13.4-201 including the FFD program.

### 13.7.3 Regulatory Basis

The applicable regulatory requirements for STD SUP 13.7-1 are as follows:

- 10 CFR Part 26, "Fitness for duty programs"
- 10 CFR 52.79(a)(44)

Regulatory guidance for FFD programs is included in RG 1.206.

### 13.7.4 Technical Evaluation

The NRC staff reviewed Section 13.7 of the VCSNS COL FSAR to ensure that the COL application represents the complete scope of information relating to this review topic.[1] The NRC staff's review confirmed that the information in the application addresses the required information relating to the FFD program.

Section 1.2.3 of this SER provides a discussion of the strategy used by the NRC to perform one technical review for each standard issue outside the scope of the DC and use this review in evaluating subsequent COL applications. To ensure that the staff's findings on standard content that were documented in the SER for the reference COL application (VEGP Units 3 and 4) were equally applicable to the VCSNS Units 2 and 3 COL application, the staff undertook the following reviews:

- The staff compared the VEGP COL FSAR, Revision 2 to the VCSNS COL FSAR. In performing this comparison, the staff considered changes made to the VCSNS COL FSAR (and other parts of the COL application, as applicable) resulting from RAIs.

- The staff verified that the site-specific differences were not relevant.

The staff has completed its review and found the evaluation performed for the standard content to be directly applicable to the VCSNS COL application. This standard content material is identified in this SER by use of italicized, double-indented formatting. Instead of confirming that all responses to RAIs identified in the corresponding standard content evaluation were endorsed by the VCSNS applicant (which is a typical step when comparing the two applications), the NRC staff provides its evaluation of similar RAIs issued to VCSNS, following the standard content material. The one confirmatory item in the standard content material retains the number assigned in the VEGP SER, and is also addressed following the standard content material.

The following portion of this technical evaluation section is reproduced from Section 13.7.4 of the VEGP SER:

> *Supplemental Information*
>
> - *STD SUP 13.7-1*
>
> *The applicant provided a new Section 13.7 in the VEGP COL FSAR describing the FFD program. STD SUP 13.7-1 added the following text to Section 13.7:*

> *The Fitness for Duty (FFD) Program (Program) is implemented and maintained in two phases; the construction phase program and the operating phase program. The construction and operations phase programs are implemented as identified in* [FSAR] *Table 13.4-201.*
>
> *The construction phase program is consistent with NEI 06-06 (*[FSAR] *Reference 201). The workforce population subject to random testing during construction is determined on a weekly basis by averaging the total number of active construction badges over each preceding seven-day period. The random selection from each week's workforce population is identified by a standard computer-generated random number generator using this number of active badges as the range of numbers considered in the weekly random testing selection.*
>
> *The operations phase program is consistent with 10 CFR Part 26.*

*The staff notes that Reference 201 in the above text refers to Revision 4 of NEI 06-06.*

*The NRC staff's review of STD SUP 13.7-1 included the following: (1) the adequacy of the FFD program for the construction phase; (2) the adequacy of the FFD program for the operations phase; and (3) the implementation schedule proposed by the applicant for both the construction phase and operations phase FFD operational programs.*

*The NRC staff issued three requests for additional information (RAIs) to obtain further clarification on the applicant's FFD Program. The first two RAIs discussed below are associated with the resolution of STD SUP 13.7-1.*

*In RAI 13.6-33, the staff asked how the applicant intends to update its FFD program for the construction phase. NEI 06-06 provides examples of the FFD program that is required and, if this guidance is endorsed by the NRC, will provide an acceptable method of complying with the NRC's regulations. If the NRC endorses NEI 06-06, does the applicant intend to update its FFD program for the construction phase to comply with NEI 06-06? If future revisions to NEI 06-06 are endorsed by the NRC, does the applicant intend to update its FFD program for the construction phase to comply with certain clarifications, additions, and exceptions in these future, endorsed revisions, as necessary?*

*The applicant replied that it submitted an FFD Program for NRC approval as part of the Limited Work Authorization (LWA) request, and that the program is now being implemented as part of the construction activities. If NEI 06-06 is endorsed by the NRC, SNC plans to transition to a program that follows the guidance in NEI 06-06. The COL application currently commits to NEI 06-06, Revision 4, and*

*will be changed in a future revision to commit to NEI 06-06, Revision 5. The applicant will evaluate substantial changes in subsequent revisions to NEI 06-06 and modify the construction phase FFD program to incorporate those substantial changes determined to be appropriate.*

*The applicant's response to RAI 13.6-33, as well as its supplemental response, revises Section 13.7 to address the issues discussed above. The relevant portion of the proposed revised text, to be included in a future revision of the VEGP COL FSAR, is included below:*

> *The Fitness for Duty Program (FFD) is implemented and maintained in multiple and progressive phases dependent on the activities, duties, or access afforded to certain individuals at the construction site. In general, two different FFD programs will be implemented: a construction FFD program and an operations FFD program. The construction and operations phase programs are illustrated in* [FSAR] *Table 13.4-201.*
>
> *The construction FFD program is consistent with NEI 06-06 (*[FSAR] *Reference 201). NEI 06-06 applies to persons constructing or directing the construction of safety- and security-related structures, systems, or components performed onsite where the new reactor will be installed and operated. Management and oversight personnel, as further described in NEI 06-06, and security personnel prior to the receipt of special nuclear material in the form of fuel assemblies (with certain exceptions) will be subject to the operations FFD program that meets the requirements of 10 CFR Part 26, Subparts A through H, N, and O. At the establishment of a protected area, all persons who are granted unescorted access will meet the requirements of an operations FFD program. Prior to issuance of a Combined License, the construction FFD program at a new reactor construction site for those subject to Subpart K will be reviewed and revised as necessary should substantial revisions occur to either NEI 06-06 following NRC endorsement or the requirements of 10 CFR Part 26.*

*The staff notes that Reference 201 in the above text refers to Revision 5 of NEI 06-06.*

*In RAI 13.6-34, the staff asked the applicant to: (1) describe how FSAR Table 13.4-201, Item 15, related to the security operational program, comports with 10 CFR 26.3 and 10 CFR 26.4, and the guidance provided in the NRC's letter to NEI dated December 2, 2009, entitled "Status of U.S. Nuclear Regulatory Commission Review and Endorsement of NEI 06-06, 'Fitness for Duty Program Guidance for New Nuclear Power Plant Construction Sites,'" and (2) provide site-specific information to clearly and sufficiently describe the applicant's FFD*

*program. This information would include, but is not limited to, any deviations or exceptions to the requirements of 10 CFR Part 26 as further described in NEI 06-06.*

*The applicant stated that the response to RAI 13.6-33 provided the changes to the COL application that will describe the FFD program required by 10 CFR Part 26. Site-specific information is also provided in that response to clarify which program will be used to cover the various classifications of workers that must be covered in accordance with 10 CFR Part 26. The applicant's response to RAI 13.6-35 (below) revises FSAR Table 13.4-201, Item 20 to address the guidance provided in the NRC's December 2, 2009 letter. The proposed revision to Item 20 of FSAR Table 13.4-201, to be included in a future revision of the VEGP COL FSAR, is included below:*

| Item | Program Title | Program Source (required by) | FSAR Section | Implementation Milestone | Implementation Requirements |
|---|---|---|---|---|---|
| 20. | Fitness for Duty (FFD) Program for Construction (workers and first-line supervisors) | 10 CFR 26.4(f) | 13.7 | Prior to initiating 10 CFR Part 26 construction activities | 10 CFR Part 26, Subpart K |
| | FFD Program for Construction (management and oversight personnel) | 10 CFR 26.4(e) | 13.7 | Prior to initiating 10 CFR Part 26 construction activities | 10 CFR Part 26, Subparts A - H, N, and O |
| | FFD Program for Security Personnel | 10 CFR 26.4(e)(1) | 13.7 | Prior to initiating 10 CFR Part 26 construction activities | 10 CFR Part 26, Subparts A - H, N, and O |
| | | 10 CFR 26.4(a)(5) or 26.4(e)(1) | | Prior to the earlier of:<br>A. Licensee's receipt of SNM in the form of fuel assemblies, or<br>B. Establishment of a protected area, or<br>C. The 10 CFR 52.103(g) finding | 10 CFR Part 26, Subparts A - I, N, and O |
| | FFD Program for FFD Program personnel | 10 CFR 26.4(g) | 13.7 | Prior to initiating 10 CFR Part 26 construction activities | 10 CFR Part 26, Subparts A, B, D - H, N, O, and C per licensee's discretion |

| Item | Program Title | Program Source (required by) | FSAR Section | Implementation Milestone | Implementation Requirements |
|---|---|---|---|---|---|
| | FFD Program for persons required to physically report to the Technical Support Center (TSC) or Emergency Operations Facility (EOF) | 10 CFR 26.4(c) | 13.7 | Prior to the conduct of the first full-participation emergency preparedness exercise under 10 CFR Part 50, App. E, Section F.2.a | 10 CFR Part 26, Subparts A - I, N, and O, except for §§ 26.205 – 209 |
| | FFD Program for Operation | 10 CFR 26.4(a) and (b) | 13.7 | Prior to the earlier of:<br>A. Establishment of a protected area, or<br>B. The 10 CFR 52.103(g) finding | 10 CFR Part 26, Subparts A - I, N, and O, except for individuals listed in § 26.4(b), who are not subject to §§ 26.205 – 209 |

*In its December 2, 2009, letter to NEI, the NRC stated that during the review and approval process for NEI 06-06, the applicant should provide the following statements in its application:*

- *NEI 06-06, Revision 5 was used in the development of the construction site FFD program.*
- *The applicant will review and revise its construction site FFD program as necessary to ensure that it comports with the NRC-endorsed version of NEI 06-06.*
- *If the NRC staff's review of NEI 06-06 results in substantive changes to the most recent, docketed FFD program description provided by the applicant, the applicant must amend its application to reflect the changes.*

*The applicant's proposed revisions to FSAR Section 13.7 satisfactorily address the three items described above. The December 2, 2009, letter also provided implementation milestones for consideration by applicants. The staff confirmed that the proposed revisions to FSAR Table 13.4-201, Item 20, include all of the implementation milestones in the December 2, 2009, letter.*

*Therefore, based on the staff's acceptance of the proposed revisions to FSAR Section 13.7 and to FSAR Table 13.4-201, Item 20, as noted above, the NRC staff concludes that the applicant has satisfactorily addressed STD SUP 13.7-1 by providing sufficient information on the FFD program for both the construction phase and the operating phase of the units. The inclusion of this information in a future revision of the VEGP COL FSAR is* ***Confirmatory Item 13.7-1****.*

*License Conditions*

*In RAI 13.6-35, the staff asked the applicant if proposed License Condition 3, A.1, and G.7, described in Part 10 of the COL application comports with FSAR Table 13.4-201, Item 15, which itemizes the aspects of the security operational program.*

*The staff further evaluated the need for License Condition 3, A.1 and G.7, for the VEGP COL application and determined it was not needed because the implementation milestones for FFD are governed by 10 CFR Part 26. The staff communicated this information to SNC, which then submitted Supplement 1 to its response to this RAI, removing this license condition for FFD.*

- *Part 10, License Condition 6*

*The applicant proposed a license condition in Part 10 of the VEGP COL application to provide a schedule to support the NRC's inspection of operational programs, including the FFD program.*

*The proposed license condition is consistent with the policy established in SECY 05-0197, "Review of Operational Programs in a Combined License Application and Generic Emergency Planning Inspections, Tests, Analyses, and Acceptance Criteria," for operational programs and is acceptable.*

Evaluation of VCSNS RAIs

The NRC staff issued RAIs to the VCSNS applicant that mirrored the RAIs issued to the VEGP applicant. Specifically, RAIs 13.6.1-1, 13.6.1-2, and 13.6.1-3 issued to the VCSNS applicant correspond to RAIs 13.6-33, 13.6-34, and 13.6-35, respectively, issued to the VEGP applicant.

The NRC staff's evaluation of the responses provided by the VCSNS applicant to the three questions related to the FFD program is discussed below. The VCSNS applicant responded to these three RAIs in a letter dated March 15, 2010, and superseded its response to RAI 13.6.1-3 in its letter dated July 1, 2010.

In response to RAI 13.6.1-1, the VCSNS applicant stated that it currently commits to NEI 06-06, Revision 4, and will change its application in a future revision to commit to NEI 06-06, Revision 5. The VCSNS applicant stated that it will evaluate substantial changes in subsequent revisions to NEI 06-06 and modify the construction phase FFD program to incorporate those substantial changes determined to be appropriate. The applicant's response to RAI 13.6.1-1 revised Section 13.7 to address the issues discussed above. The relevant portion of the proposed revised text, to be included in a future revision of the VCSNS COL FSAR, is included below:

> The Fitness for Duty Program (FFD) is implemented and maintained in multiple and progressive phases dependent on the activities, duties, or access afforded to certain individuals at the construction site. In general, two different FFD

> programs will be implemented: a construction FFD program and an operations FFD program. The construction and operations phase programs are illustrated in Table 13.4-201.
>
> The construction FFD program is consistent with NEI 06-06 ([FSAR] Reference 201). NEI 06-06 applies to persons constructing or directing the construction of safety- and security- related structures, systems, or components performed onsite where the new reactor will be installed and operated. Management and oversight personnel, as further described in NEI 06-06, and security personnel prior to the receipt of special nuclear material in the form of fuel assemblies (with certain exceptions) will be subject to the operations FFD program that meets the requirements of 10 CFR Part 26, Subparts A through H, N, and 0. At the establishment of a protected area, all persons who are granted unescorted access will meet the requirements of an operations FFD program. Prior to issuance of a Combined License, the construction FFD program at a new reactor construction site for those subject to Subpart K will be reviewed and revised as necessary should substantial revisions occur to either NEI 06-06 following NRC endorsement or the requirements of 10 CFR Part 26.

In response to RAI 13.6.1-2, the VCSNS applicant stated that the response to RAI 13.6.1-1 provides the changes to the COL application that will describe the FFD program required by 10 CFR Part 26. The site-specific information is also provided in that response to clarify which program will be used to cover the various classifications of workers that must be covered in accordance with 10 CFR Part 26. The response to RAI 13.6.1-3 provides the information on modifications to VCSNS COL FSAR Table 13.4-201, Item 20 to address the guidance provided in the NRC's December 2, 2009, letter to NEI. That RAI response includes changes to License Condition 3, Items A, C, and D in Part 10 of the COL application to align with the changes to VCSNS COL FSAR Table 13.4-201. The NRC staff verified that the proposed changes to VCSNS COL FSAR Table 13.4-201, Item 20 are identical to the proposed changes to the corresponding VEGP COL FSAR Table 13.4-201, which is provided in the standard content evaluation material above.

In response to RAI 13.6.1-3, the VCSNS applicant stated that it would remove from proposed License Condition 3 any reference to implementation milestones for the FFD program, since these implementation requirements are in the applicable NRC regulations.

The NRC staff compared the responses provided by the VCSNS applicant to the responses provided by the VEGP applicant, and concluded that the responses are essentially identical, after accounting for the differences of an Early Site Permit having been issued for the VEGP site for this issue. Therefore, the conclusions reached by the NRC staff regarding the FFD program at VEGP are applicable to the FFD program at VCSNS. The inclusion of the information provided in the RAI responses in a future revision of the VCSNS COL FSAR is part of **Confirmatory Item 13.7-1** that is discussed in the standard content portion of this safety evaluation above.

### 13.7.5 Post Combined License Activities

For the reasons discussed in the technical evaluation section above, the staff proposes to include the following license conditions to address the FFD program details:

- License Condition (13-6) - The licensee shall submit to the Director of NRO, a schedule, no later than 12 months after issuance of the COL, that supports planning for and conduct of NRC inspection of the FFD operational program. The schedule shall be updated every 6 months until 12 months before scheduled fuel load, and every month thereafter until either the FFD operational program has been fully implemented or the plant has been placed in commercial service, whichever comes first.

### 13.7.6 Conclusion

The NRC staff's review confirmed that the applicant addressed the required information relating to the FFD program and there is no outstanding information to be addressed in the VCSNS COL FSAR related to this section.

Pending closure of **Confirmatory Item 13.7-1**, the staff concludes that the information presented in the VCSNS COL FSAR is acceptable because it meets the regulatory requirements in 10 CFR Part 26 and 10 CFR 52.79(a)(44). The staff based its conclusion on the following:

- STD SUP 13.7-1, relating to the FFD program, is acceptable because it meets 10 CFR Part 26 and 10 CFR 52.79(a)(44).

## 13.8 Cyber Security

### 13.8.1 Introduction

In a letter to the NRC, dated June 22, 2010, SCE&G submitted Revision 0 of the CSP for VCSNS Units 2 and 3. The CSP applies to all critical digital assets required for VCSNS operation. In the submittal, the applicant describes how the requirements of 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks" (the rule) will be implemented to protect digital computer and communications systems and networks associated with the following functions from those cyber attacks, up to and including the design-basis threat (DBT) described in 10 CFR 73.1, "Purpose and Scope." The scope of 10 CFR 73.54 includes critical digital assets (CDAs) associated with the following:

- safety-related and important-to-safety functions
- security functions
- emergency preparedness functions, including offsite communications
- support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions

### 13.8.2 Summary of Application

The applicant addresses cyber security in Section 13.6 of the VCSNS COL FSAR. Section 13.6 of the VCSNS COL FSAR, Revision 2, incorporates by reference Section 13.6 of the AP1000 DCD, Revision 17. The applicant's CSP includes deviations from RG 5.71, "Cyber Security Programs for Nuclear Facilities." The staff has evaluated these deviations.

In addition, in VCSNS COL FSAR Section 13.6, the applicant provides the following:

*AP1000 COL Information Item*

- STD COL 13.6-5

The applicant provided additional information in STD COL 13.6-5 to address COL Information Item 13.6-5, which provides information related to the cyber security program.

*License Conditions*

- Part 10, License Condition 3, Item G.10

The applicant proposed a license condition in Part 10 of the VCSNS COL application requiring the applicant to implement the cyber security program prior to initial fuel load.

- Part 10, License Condition 6

The applicant proposed a license condition in Part 10 of the VCSNS COL application to provide a schedule to support the NRC's inspection of operational programs included in VCSNS COL FSAR Table 13.4-201 including the cyber security program.

### 13.8.3 Regulatory Basis

The regulatory basis of the information incorporated by reference is addressed in NUREG-1793 and its supplements.

The applicable regulatory requirements for cyber security are as follows:

- 10 CFR 73.1, "Purpose and scope"
- 10 CFR 73.54, "Protection of digital computer and communication systems and networks"
- 10 CFR 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage," paragraphs (a)(1), (b)(8), and (m)
- 10 CFR 73.58, "Safety/security interface requirements for nuclear power reactors"

- 10 CFR Part 73, "Physical protection of plants and materials," Appendix G, "Reportable Safeguards Events"

The applicable regulatory guidance for cyber security is RG 5.71.

### 13.8.4 Technical Evaluation

The NRC staff reviewed Section 13.6 of the VCSNS COL FSAR and checked the referenced DCD to ensure that the combination of the DCD and the COL application represents the complete scope of information relating to this review topic.[2] The NRC staff's review confirmed that the information in the application and incorporated by reference addresses the required information relating to cyber security. The results of the NRC staff's evaluation of the information incorporated by reference in the VCSNS COL application are documented in NUREG-1793 and its supplements.

The staff's review of the VCSNS CSP has focused on ensuring that the necessary programmatic elements are included in these plans to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety. The staff reviewed the VCSNS CSP to assure the necessary programmatic elements that, when effectively implemented, will provide the required high assurance of adequate protection. Effective implementation is dependent on the procedures and practices the applicant develops to satisfy the programmatic elements of its CSP. The facility implementing procedures are subject to future NRC inspection.

Section 1.2.3 of this SER provides a discussion of the strategy used by the NRC to perform one technical review for each standard issue outside the scope of the DC and use this review in evaluating subsequent COL applications. To ensure that the staff's findings on standard content that were documented in the SER for the reference COL application (VEGP Units 3 and 4) were equally applicable to the VCSNS Units 2 and 3 COL application, the staff undertook the following reviews:

- The staff compared the VEGP COL FSAR, Revision 2 to the VCSNS COL FSAR. In performing this comparison, the staff considered changes made to the VCSNS COL FSAR (and other parts of the COL application, as applicable) resulting from RAIs.

- The staff confirmed that the June 22, 2010, VCSNS submittal transmitting its CSP was identical to the June 14, 2010, VEGP submittal transmitting its CSP, with the only exceptions being to the title of the units and the identification of the position charged with oversight of the program.

- The staff verified that the site-specific differences were not relevant.

[2] See Section 1.2.2 for a discussion of the staff's review related to verification of the scope of information to be included in a COL application that references a DC.

The staff has completed its review and found the evaluation performed for the standard content to be directly applicable to the VCSNS COL application. This finding included verifying that the difference in the position charged with oversight of the program (the General Manager, Organizational Effectiveness at VCSNS and Vice President of Nuclear Operations Support at VEGP) does not affect the staff's conclusions regarding the applicant's CSP. This standard content material is identified in this SER by use of italicized, double-indented formatting. The one confirmatory item in the standard content material retains the number assigned in the VEGP SER.

The following portion of this technical evaluation section is reproduced from Section 13.8.4 of the VEGP SER:

*AP1000 COL Information Item*

- *STD COL 13.6-5*

*The NRC staff reviewed STD COL 13.6-5 related to COL Information Item 13.6-5, which identifies the need for a COL applicant to address cyber security. STD COL 13.6-5 supplemented Section 13.6 of the VEGP COL FSAR by stating the following text is to be added after Section 13.6 of the VEGP ESP SSAR:*

> *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.*

*Section 13.6 of the VEGP COL FSAR also refers to FSAR Table 13.4-201, "Operational Programs Required by NRC Regulations," as providing the milestone for implementing the cyber security program.*

*The VEGP applicant submitted its Revision 0 of its CSP in a letter dated June 14, 2010, to demonstrate that the cyber security program will provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the DBT as described in 10 CFR 73.1. The CSP has been withheld from public disclosure pursuant to 10 CFR 2.390(d)(1). In its review of this plan, the NRC staff used the guidance in RG 5.71 to determine if the regulatory requirements described in Section 13.8.3 of this SER are satisfied.*

*The applicant described the cyber security program based on 10 CFR 73.54, including the audit of the effectiveness of the cyber security program as required by 10 CFR 73.55(m), submittal of CSPs and the establishment, maintenance and implementation of a cyber security program required by 10 CFR 73.55(a)(1) and 10 CFR 73.55(b)(8) and reporting requirements in 10 CFR Part 73, Appendix G.*

*The implementation milestones for this program are included in VEGP COL FSAR Table 13.4-201.*

*As detailed in the remainder of this SER section, the CSP has been reviewed by the NRC staff for format and content utilizing the NRC CSP template in RG 5.71, and found to include all features considered essential for such a program, and is acceptable. In particular, it has been found to comply with the Commission's regulations including 10 CFR 73.54, 10 CFR 73.55(a)(1), 10 CFR 73.55(b)(8), 10 CFR 73.55(m), and 10 CFR Part 73, Appendix G and conforms to the NRC CSP template set forth in RG 5.71.*

*The applicant has committed to incorporate this CSP into a future revision of the VEGP COL application to address NRC requirements in 10 CFR 73.54. This action will be tracked as* ***Confirmatory Item 13.8-1.***

*13.8.4.1 Establishment of Cyber Security Program*

*The VEGP CSP describes how SNC will establish a cyber security program to achieve high assurance that the VEGP digital computer and communication systems and networks associated with safety, security, and emergency preparedness, including offsite communications and support systems and equipment which if compromised would adversely impact safety, security and/or emergency preparedness (SSEP) functions, and their digital assets, hereafter defined as CDAs, are adequately protected against cyber attacks up to and including the DBT. RG 5.71 provides a method that the staff considers acceptable for complying with this regulation. SNC complies with the requirements of 10 CFR 73.54 by providing a CSP that follows the template in Appendix A of RG 5.71, except as noted in Attachment A, "Vogtle Electric Generating Plant Units 3 and 4 Cyber Security Plan Deviations from Regulatory Guide RG 5.71."*

*The NRC staff reviewed the VEGP CSP against the template in RG 5.71.*

*The applicant states in the VEGP CSP that its security program complies with 10 CFR 73.54 by:*

*(1) establishing and implementing defensive strategies consistent with the defensive model, described in Section 3.1.5, including the security controls described in Sections 3.1, 3.2, and 3.3.*

*(2) maintaining the program, as described in Section A.4.*

*Based on the above review, the NRC staff finds that establishment of a cyber security program described in Section 1 of the VEGP CSP is acceptable.*

*The following SER Sections 13.8.4.2 through 13.8.4.23 correlate to specific sections in Appendix A to RG 5.71. These SER sections use the same headings*

*as the corresponding Appendix A sections, and include the Appendix A numbering system in the titles. SER Section 13.8.4.24 addresses each of the deviations identified in the applicant's CSP.*

*13.8.4.2 Security Assessment and Authorization (Section A.3.1.1 of Appendix A to RG 5.71)*

*Section 3.1.1 of the VEGP CSP states that the following will be reviewed every 24 months:*

- *A formal documented security planning, assessment, and authorization policy that describes the purpose, scope, roles, responsibilities, management commitments, and coordination among departments and the implementation of the security program and the controls applied in accordance with Section 3.1.6*

- *A formal documented procedure to facilitate the implementation of the cyber security program and the security assessment*

*The NRC staff reviewed the above and found that evaluation of the program elements every 24 months is not consistent with Section C.3.1.1 of RG 5.71. The time period between evaluations is 12 months longer than the time period provided in brackets in RG 5.71. However, this 24-month time period conforms to 10 CFR 73.54(g), requiring the applicant to review the cyber security program as a component of the physical security program in accordance with the requirements of 10 CFR 73.55(m), including the periodicity requirements. The requirement of 10 CFR 73.55(m) is that at minimum the applicant review each element of the physical protection program at least every 24 months.*

*Based on the above review, the NRC staff finds that the security assessment and authorization described in Section 3.1.1 of the VEGP CSP is acceptable.*

*13.8.4.3 Cyber Security Team (Section A.3.1.2 of Appendix A to RG 5.71)*

*Section 3.1.2 of the VEGP CSP states that a cyber security team, composed of individuals with broad knowledge, will be established and maintained and that the broad knowledge of the team will include the following areas:*

- *Information and digital system technology; this includes cyber security, software development, offsite communications, computer system administration, computer engineering, and computer networking.*

- *Nuclear facility operations, engineering, and safety; this includes overall facility operations and plant technical specification compliance.*

- *Physical security and emergency preparedness; this includes the site's physical security and emergency preparedness systems and programs.*

*This section of the VEGP CSP also enumerates the roles and responsibilities of the cyber security team. Aside from the deviations discussed below, this section of the VEGP CSP conforms to the CSP template wording provided in Section A.3.1.2 of RG 5.71.*

*The VEGP CSP includes several deviations from the text of RG 5.71:*

1) *The first deviation clarifies that the cyber security team (CST) will be responsible for "overseeing" preparation of documentation of cyber security controls and that, in fact, non-team members (such as vendor personnel) may perform some of these actions, under the supervision of the CST. This clarification is acceptable to the staff since the responsibility to ensure compliance with 10 CFR 73.54 remains with the CST.*

2) *The second deviation changes the CST responsibility from "assuring the retention" of assessment documentation to "establishing the retention policy" for assessment documentation. Again, the deviation is acceptable to the staff since the responsibility to ensure compliance with 10 CFR 73.54 remains with the CST.*

3) *The third and final deviation seeks to change the basis for CST determinations being made in a free and objective manner. The RG 5.71 wording states that the CST should be free to make determinations that are not constrained by "operational goals." The deviation changes the respective sentence to say "…by business goals." Again, the deviation is acceptable to the staff since it maintains the same objective of keeping financial considerations out of decision making regarding cyber security.*

*Based on the above review, the NRC staff finds that the CST described in Section 3.1.2 of the VEGP CSP is acceptable.*

*13.8.4.4 <u>Identification of Critical Digital Assets (Section A.3.1.3 of Appendix A to RG 5.71)</u>*

*Section 3.1.3 of the VEGP CSP states that to identify the critical systems (CSs) at VEGP, the CST identified and documented plant systems, equipment, communication systems, and networks that are associated with the SSEP functions described in 10 CFR 73.54(a)(1), as well as the support systems associated with these SSEP functions in accordance with the approved plant licensing basis.*

*The VEGP CSP also states that the CST identified and documented CDAs that have a direct, supporting, or indirect role in the proper functioning of CSs.*

*The steps outlined in the VEGP CSP essentially match the corresponding steps described in RG 5.71 for this same activity. The only difference between the corresponding section in RG 5.71 and the VEGP CSP is the addition of the modifying phrase: "…and defined in the approved plant licensing basis."*

*10 CFR 73.54(a)(1) requires that the licensee 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 SSEP functions.*

*This deviation is acceptable because SNC proposes to use its licensing basis to identify CSs that are associated with SSEP functions, as 10 CFR 73.54 requires. This statement includes the first step in RG 5.71 to analyze digital computer and communication systems and networks to determine if they include CDAs.*

*Based on the above review, the NRC staff finds the applicant's proposal, described in Section 3.1.3 of the VEGP CSP, to use 10 CFR 73.54(a)(1) and its licensing basis to identify CDAs to be acceptable.*

*13.8.4.5 Reviews and Validation Testing (Section A.3.1.4 of Appendix A to RG 5.71)*

*Section 3.1.4 of the VEGP CSP states that the VEGP CST will be responsible for conducting a review, performing validation activities, and for each CDA, the CST determined:*

- *its direct and indirect connectivity pathways*
- *infrastructure interdependencies*
- *the application of defensive strategies, including defensive models, security controls, and other defensive measures*

*The CSP also requires that the CST validate the above activities through comprehensive walkdowns, which include a range of activities that conform to those activities specified in RG 5.71 for this purpose.*

*The requirements, processes and procedures described in this section of the VEGP CSP conform to, and encompass all of the same specifications, outlined in the comparable section of RG 5.71.*

*Based on the above review, the NRC staff finds that reviews and validation testing described in Section 3.1.4 of the VEGP CSP is acceptable.*

*13.8.4.6 Defense-In-Depth Protective Strategies (Section A.3.1.5 of Appendix A to RG 5.71)*

*Section 3.1.5 of the VEGP CSP states that the defensive strategy consists of the defensive model described in Section C.3.2 of RG 5.71, and the detailed defensive architecture of Appendix C, Section 6, defense-in-depth controls in Appendix C, Section 7, and security controls applied in accordance with Section 3.1.6 of the VEGP CSP with one deviation to its defensive architecture. The VEGP defensive architecture, including the deviation is consistent with the security model described in RG 5.71, which provides for isolation of safety-related and security CDAs.*

*Based on the above review, the NRC staff finds that the defense-in-depth protective strategies described in Section 3.1.5 of the VEGP CSP are acceptable.*

*13.8.4.7 Application of Security Controls (Section A.3.1.6 of Appendix A to RG 5.71)*

*Section 3.1.6 of the VEGP CSP states that VEGP Units 3 and 4 established defense-in-depth protective strategies by applying and documenting the following:*

- *the defensive model described in Section 3.2 of RG 5.71 (discussed in SER Section 13.8.4.6)*
- *the physical and administrative security controls established by the VEGP Units 3 and 4 Physical Security Program and physical barriers, such as locked doors, locked cabinets, and locating CDAs in the VEGP Units 3 and 4 protected area or vital area*[s]*, which are part of the overall security controls used to protect CDAs from attacks*
- *verification of the effectiveness of the implemented operational and management controls described in Appendix C to RG 5.71 and implemented alternatives to the Appendix C controls for each CDA*
- *the technical controls described in Appendix B to RG 5.71 and the operational and management controls described in Appendix C to RG 5.71, consistent with the process described below*

*The VEGP CSP deviates from RG 5.71, Section C.3.3 Security Controls and Appendix A.3.1.6, by stating that when a control from Appendices B and C of RG 5.71 is not implemented, the licensee will implement alternate control(s) that "do not provide less protection that the corresponding" control in the appendix. This deviation is consistent with the method used in RG 5.71, which states that controls should provide equal or better protection.*

*The VEGP CSP also deviates from RG 5.71 by stating that when a control can be proved to be unnecessary, the applicant will perform an analysis demonstrating that the control is not necessary, and will provide a documented justification. Although RG 5.71 specifically calls for an attack vector analysis, and the VEGP CSP does not specifically commit to performing an attack vector analysis, the VEGP CSP does commit to justifying the non-applicability of a control by demonstrating that the attack vector does not exist. This provides for the same outcome as RG 5.71.*

*Based on the above review, the NRC staff finds that the application of security controls described in Section 3.1.6 of the VEGP CSP is acceptable.*

*13.8.4.8 Incorporating the Cyber Security Program into the Physical Protection Program (Section A.3.2 of Appendix A to RG 5.71)*

*Section 3.2 of the VEGP CSP states that the licensee will provide the management interfaces necessary to appropriately coordinate physical and cyber security activities, as follows:*

- *establish an organization that is responsible for cyber security and is independent from operations*
- *document physical and cyber security interdependencies*
- *develop policies and procedures to coordinate management of physical and cyber security controls*
- *incorporate unified policies and procedures to secure CDAs from attacks up to and including the DBT*
- *coordinate acquisition of physical or cyber security services, training, devices, and equipment*
- *coordinate interdependent physical and cyber security activities and training with physical and cyber security personnel*
- *integrate and coordinate incident response capabilities with physical and cyber incident response personnel*
- *train senior management regarding the needs of both disciplines*
- *periodically exercise the entire security organization using realistic scenarios combining both physical and cyber simulated attacks*

*The VEGP CSP deviates from RG 5.71 by not creating a unified security organization. The commitment to provide for appropriate management interfaces*

*to coordinate the physical and cyber security organizations provides for a level of integration equivalent to a unified organization.*

*Based on the above review, the NRC staff finds that the incorporation of the cyber security program into the physical protection program described in Section 3.2 of the VEGP CSP is acceptable.*

*13.8.4.9 Policies and Implementing Procedures (Section A.3.3 of Appendix A to RG 5.71)*

*Section 3.3 of the VEGP CSP states that the licensee will develop policies and procedures to address the security controls in Appendices B and C to RG 5.71 and review and approve issues and uses, and revise the same according to Section 4 of the CSP. The CSP will also establish specific responsibilities for the positions described in Section 10.10 of Appendix C to RG 5.71, with the following deviation.*

*The CSP states that this will occur "in accordance with the security control application process in Section 3.1.6 of this Plan." This process requires the applicant to justify and demonstrate that any deviation from the controls in RG 5.71 provide no less protection than the corresponding control in Appendices B and C; therefore, the VEGP CSP will require the same level of protection as the corresponding commitment in RG 5.71.*

*Based on the above review, the NRC staff finds that the policies and implementing procedures described in Section 3.3 of the VEGP CSP are acceptable.*

*13.8.4.10 Maintaining the Cyber Security Program (Section A.4 of Appendix A to RG 5.71)*

*Section 4 of the VEGP CSP states that the applicant will establish the programmatic elements necessary to maintain security throughout the life cycle of the CDAs, and that the applicant has implemented these elements. For new assets, SNC commits to follow the process described in Section 4.2.*

*Section 4 of the VEGP CSP is nearly identical to Section C.4 of RG 5.71, with the deviation of replacing the bracketed text* [Licensee/Applicant] *with VEGP Units 3 and 4, and by including the caveat that the operational and management controls are applied following the process described in Section 3.1.6. The process described in Section 3.1.6 allows the licensee/applicant to not apply a control if it can demonstrate that the control is not necessary by justifying that the attack vector associated with the control does not exist. This approach is consistent with the method used in RG 5.71, and does not reduce the protection to the plant.*

*Based on the above review, the NRC staff finds that the maintenance of the cyber security program described in Section 4 of the VEGP CSP is acceptable.*

*13.8.4.11 Continuous Monitoring and Assessment (Section A.4.1 of Appendix A to RG 5.71)*

*Section 4.1 of the VEGP CSP states that the licensee will continue to monitor security controls for effectiveness; will ensure that they remain in place throughout the life cycle of the CDA; and will verify that rogue assets are not connected to the infrastructure.*

*The VEGP CSP includes a single deviation from Section A.4.1 of RG 5.71. The RG states that "*[Licensee/Applicant] *continuously monitors security controls consistent with Appendix C to RG 5.71," whereas the VEGP CSP states that "VEGP Units 3 and 4 continues to monitor security controls consistent with Appendix C to RG 5.71."*

*This deviation is consistent with the method in RG 5.71, which calls for periodic assessments, which is consistent with the statement "continues to monitor."*

*Based on the above review, the NRC staff finds that the ongoing monitoring and assessment described in Section 4.1 of the VEGP CSP is acceptable.*

*13.8.4.12 Periodic Assessment of Security Controls (Section A.4.1.1 of Appendix A to RG 5.71)*

*Section 4.1.1 of the VEGP CSP states that the licensee will periodically assess that security controls implemented for each CDA remain robust, resilient, and effective in place throughout the life cycle, at least every 24 months.*

*The NRC staff reviewed the above and found that this period of assessment is not consistent with RG 5.71. The time period between evaluations is 12 months longer than the time period provided in RG 5.71. However, this 24-month time period conforms to 10 CFR 73.54(g) requiring the licensee/applicant to review the cyber security program as a component of the physical security program in accordance with the requirements of 10 CFR 73.55(m), including the periodicity requirements. The requirements of 10 CFR 73.55(m) are that, at a minimum, the licensee/applicant review each element of the physical protection program, which includes the cyber security program, at least every 24 months.*

*Furthermore, the VEGP CSP states that controls will be reviewed according to the requirements of the security controls if that period of review occurs more often. This is also consistent with the method provided in RG 5.71.*

*Based on the above review, the NRC staff finds that the periodic assessment of security controls described in Section 4.1.1 of the VEGP CSP is acceptable.*

*13.8.4.13 Effectiveness Analysis (Section A.4.1.2 of Appendix A to RG 5.71)*

*Section 4.1.2 of the VEGP CSP states that the licensee will monitor and measure the effectiveness of the cyber security program and its security controls to ensure that both are implemented correctly, operating as intended, and continuing to provide high assurance that CDAs are protected against cyber attacks. The licensee commits to verifying the effectiveness of the security controls every 24 months, or in accordance with the specific requirements of the implemented security controls, whichever is more frequent.*

*The NRC staff reviewed the above and found that this period of verification is inconsistent with RG 5.71. The time period between evaluations is 12 months longer than the time period provided in RG 5.71. However, this 24-month time period conforms to 10 CFR 73.54(g) requiring the applicant to review the cyber security program as a component of the physical security program in accordance with the requirements of 10 CFR 73.55(m), including the periodicity requirements. The requirements of 10 CFR 73.55(m) are that, at a minimum, the applicant review each element of the physical protection program, which includes the cyber security program, at least every 24 months.*

*Furthermore, the VEGP CSP states that verification will also occur according to the requirements of the security controls if that period of verification occurs more often. This is also consistent with the method provided in RG 5.71.*

*Based on the above review, the NRC staff finds that the effectiveness analysis described in Section 4.1.2 of the VEGP CSP is acceptable.*

*13.8.4.14 Vulnerability Assessments and Scans (Section A.4.1.3 of Appendix A to RG 5.71)*

*Section 4.1.3 of the VEGP CSP states vulnerability assessments will be performed as specified in the security controls in Appendices B and C of RG 5.71 to identify new vulnerabilities that have the potential to impact the effectiveness of the cyber security program and the security of the CDAs. The applicant also commits to address vulnerabilities that could cause CDAs to become compromised or could have an adverse impact on SSEP functions. Section 13.1 of Appendix C of RG 5.71 provides that vulnerability assessments should occur no less frequently than once a quarter, at random intervals, and when new potential vulnerabilities are reported and identified.*

*Section A.4.1.3 of RG 5.71 states that vulnerability assessments will occur no less frequently than quarterly, whereas the VEGP CSP states that this will occur, "as specified in the implemented security controls in Appendices B and C to RG 5.71 and implemented alternatives to the Appendices B and C controls." The process SNC has committed to in Section 3.1.6 of the VEGP CSP requires SNC, if it does not implement the controls in Appendices B and C, to demonstrate that*

*an alternate control does not provide less protection than the corresponding control in Appendices B and C.*

*Therefore, if SNC does not implement the security control in Section 13.1, or deviates from the requirement for a quarterly vulnerability assessment, it will ensure that this deviation does not provide less protection than performing quarterly vulnerability assessments, and will provide an analysis that demonstrates that the attack vector does not exist and will document this justification for inspection.*

*Based on the above review, the NRC staff finds that the vulnerability assessments and scans described in Section 4.1.3 of the VEGP CSP are acceptable.*

*13.8.4.15 Change Control (Section A.4.2 of Appendix A to RG 5.71)*

*Section 4.2 of the VEGP CSP states that the licensee will systematically plan, approve, test, and document changes to the environment of the CDAs, the addition of CDAs to the environment, and changes to existing CDAs in a manner that provides a high level of assurance that the SSEP functions are protected from cyber attacks. The CSP also commits that the program establish that changes made to CDAs use the design control and configuration management procedures or other procedural processes to ensure that the existing security controls are effective and that any pathway that can be exploited to compromise a CDA is protected from cyber attacks.*

*The VEGP CSP does not deviate from Section A.4.2 of RG 5.71.*

*Based on the above review, the NRC staff finds that the change control process described in Section 4.2 of the VEGP CSP is acceptable.*

*13.8.4.16 Configuration Management (Section A.4.2.1 of Appendix A to RG 5.71)*

*Section 4.2.1 of the VEGP CSP states that the licensee will implement and document a change management process as described in Section 4.2 of the VEGP CSP. Further, it commits to implement and document the applied configuration management controls described in Appendix C, Section 11 to RG 5.71 following the process described in Section 3.1.6 of the CSP.*

*The VEGP CSP does not specifically commit to apply the security controls in Section 11 to Appendix C of RG 5.71; however, it does commit to apply the process in Section 3.1.6 of the CSP. The commitment in Section 4.2.1 is consistent with Section A.4.2.2 of RG 5.71 as the applicant has committed, if it does not implement the security controls in Section 11 of RG 5.71, either to implement alternative controls that do not provide less protection than what is in Section 11, or to demonstrate that this control is unnecessary by demonstrating*

*that the attack vectors associated with Section 11 to Appendix C of RG 5.71 do not exist for VEGP.*

*Based on the above review, the NRC staff finds that the configuration management process described in Section 4.2.1 of the VEGP CSP is acceptable.*

*13.8.4.17 Security Impact Analysis of Changes and Environment (Section A.4.2.2 of Appendix A to RG 5.71)*

*Section 4.2.2 of the VEGP CSP states that the applicant will perform a security impact analysis in accordance with Section 4.1.2 before implementing a design or configuration change to a CDA or, when changes to the environment occur, to manage potential risks introduced by the changes. The CSP also commits to evaluate, document, and incorporate into the security impact analysis safety and security interdependencies of other CDAs or systems, as well as updates, and documents the following:*

- *the location of the CDA and connected assets*
- *connectivity pathways (direct and indirect)*
- *infrastructure interdependencies*
- *application of defensive strategies, including defensive models, security controls, and others*
- *defensive strategy measures*
- *plant-wide physical and cyber security policies and procedures that secure CDAs from a cyber attack, including attack mitigation and incident response and recovery*

*The VEGP CSP commits to perform these impact analyses as part of the change approval process to assess the impacts of the changes on the security posture of CDAs and security controls, as described in Section 4.1.2 of the VEGP CSP, and to address any identified gaps to protect CDAs from cyber attack, up to and including the DBT as described in Section 4.2.6.*

*Finally, Section 4.2.2 states that the licensee will manage CDAs for the cyber security of SSEP functions through an ongoing evaluation of threats and vulnerabilities and implementation of each of the applied security controls provided in Appendix B or C of RG 5.71 and implement alternatives to the Appendices B and C controls during all phases of the life cycle. Additionally, SNC has established and documented procedures for screening, evaluating, mitigating, and dispositioning threat and vulnerability notifications received from credible sources. Dispositioning includes implementation of security controls to mitigate newly reported or discovered threats and vulnerabilities.*

*The language in Section 4.2.2 of the VEGP CSP is identical to that in Section A.4.2.2 of RG 5.71 and includes no deviations.*

*Based on the above review, the NRC staff finds that the security impact analysis of changes and environment described in Section 4.2.2 of the VEGP CSP is acceptable.*

*13.8.4.18 Security Reassessment and Authorization (Section A.4.2.3 of Appendix A to RG 5.71)*

*Section 4.2.3 of the VEGP CSP states that the licensee will have implemented, documented, and maintained a process that ensures that modifications to CDAs are evaluated before implementation so that security controls remain effective and that any pathway that can be exploited to compromise the modified CDA is addressed to protect CDAs and SSEP functions from cyber attacks. This section further states that the VEGP cyber security program establishes that additions and modifications are evaluated, using a proven and accepted method, before implementation to provide high assurance of adequate protection against cyber attacks, up to and including DBTs, using the process described in Section 4.1.2 of the VEGP CSP.*

*The licensee also commits to disseminate, review, and update the following when a CDA modification is conducted:*

- *a formal, documented security assessment and authorization policy, which addresses the purpose, scope, roles, responsibilities, management commitment, coordination among entities, and compliance to reflect all modifications or additions*

- *a formal, documented procedure to facilitate the implementation of the security reassessment and authorization policy and associated controls*

*The VEGP CSP does not deviate from Section A.4.2.3 of RG 5.71.*

*Based on the above review, the NRC staff finds that the security reassessment and authorization described in Section 4.2.3 of the VEGP CSP is acceptable.*

*13.8.4.19 Updating Cyber Security Practices (Section A.4.2.4 of Appendix A to RG 5.71)*

*Section 4.2.4 of the VEGP CSP states that the licensee reviews, updates and modifies cyber security policies, procedures, practices, existing cyber security controls, detailed descriptions of network architecture (including logical and physical diagrams), information on security devices, and any other information associated with the state of the cyber security program or the applied security controls provided in Appendices B and C to RG 5.71 and implemented*

*alternatives to the Appendices B and C controls when changes occur to CDAs or the environment.*

*This information includes the following:*

- *plant- and corporate-wide information on the policies, procedures, and current practices related to cyber security*
- *detailed network architectures and diagrams*
- *configuration information on security devices or CDAs*
- *new plant- or corporate-wide cyber security defensive strategies or security controls being developed and policies, procedures, practices, and technologies related to their deployment*
- *the site's physical and operational security program*
- *cyber security requirements for vendors and contractors*
- *identified potential pathways for attacks*
- *recent cyber security studies or audits (to gain insight into areas of potential vulnerabilities); and identified infrastructure support systems (e.g., electrical power; heating, ventilation, and air conditioning; communications; fire suppression) whose failure or manipulation could impact the proper functioning of CSs*

*The VEGP CSP does not deviate from Section A.4.2.4 of RG 5.71.*

*Based on the above review, the NRC staff finds that updating of cyber security practices described in Section 4.2.4 of the VEGP CSP is acceptable.*

*13.8.4.20 Review and Validation Testing of a Modification or Addition of a Critical Digital Asset (Section A.4.2.5 of Appendix A to RG 5.71)*

*The VEGP CSP Section 4.2.5 states the licensee will conduct and document the results of reviews and validation tests of each CDA modification and addition using the process described in Section 3.1.4 of the VEGP CSP.*

*The VEGP CSP does not deviate from Section A.4.2.5 of RG 5.71.*

*Based on the above review, the NRC staff finds that the Review and Validation Testing of Modifications or Additions of a Critical Digital Asset described in Section 4.2.5 of VEGP CSP is acceptable.*

*13.8.4.21 Application of Security Controls Associated with a Modification or Addition (Section A.4.2.6 of Appendix A to RG 5.71)*

*Section 4.2.6 of the VEGP CSP states that when new CDAs are introduced into the environment of VEGP, the licensee:*

- *deploys the CDA into the appropriate level of the defensive model described in Section 3.1.5 of this plan;*
- *applies the technical controls identified in Appendix B to RG 5.71 and the operational and management controls described in Appendix C to RG 5.71 in a manner consistent with the process described in Section 3.1.6 of this plan*
- *confirms that the implemented operational and management controls described in Appendix C to RG 5.71, and implemented alternatives to the Appendix C controls, are effective for the CDA*

*The plan also commits that when CDAs are modified, the licensee:*

- *verifies that the CDA is deployed into the proper level of the defensive model described in Section 3.1.5 of this plan*
- *performs a security impact analysis, as described in Section 4.2.2 of this plan*
- *verifies that the technical controls identified in Appendix B to RG 5.71 and the operational and management controls described in Appendix C to RG 5.71 are addressed in a manner consistent with the process described in Section 3.1.6 of this plan*
- *verifies that the applied security controls discussed above are implemented effectively, consistent with the process described in Section 4.1.2 of this plan*
- *confirms that the implemented operational and management controls discussed in Appendix C to RG 5.71 and implemented alternatives to the Appendix C controls are effective for the CDA*

*The VEGP CSP deviates from Section 4.2.6 of RG 5.71 by modifying the phrase "applies the technical controls identified in Appendix B to RG 5.71 in a manner consistent with the process described in Section 3.2 of RG 5.71," to read "applies the technical controls identified in Appendix B to RG 5.71 and the operational and management controls described in Appendix C to RG 5.71 in a manner consistent with the process described in Section 3.1.6 of this plan." This is consistent with RG 5.71 as the VEGP CSP commits to following the process in Section 3.1.6 of the VEGP CSP, which requires that controls are applied, an*

*alternative that provides equivalent protection is provided, or the licensee demonstrates that the control is not necessary.*

*The VEGP CSP also deviates from Section A.4.2.6 of RG 5.71 with the modification of this phrase, "verifies that the security controls discussed above are implemented effectively, consistent with the process described in Section 4.1.2 of this plan" to read "verifies that the applied security controls discussed above are implemented effectively, consistent with the process described in Section 4.1.2 of this plan."*

*This deviation is consistent with the method used in RG 5.71. RG 5.71 assumes that all the controls in Appendices B and C will be applied; whereas, the VEGP CSP commits that if a control is not applied, there will be no reduction in protection as compared to the corresponding control. This method is also captured in RG 5.71 and, therefore, the VEGP CSP is consistent with RG 5.71.*

*Based on the above review, the NRC staff finds that the application of security controls associated with a modification or addition described in Section 4.2.6 of the VEGP CSP is acceptable.*

*13.8.4.22 Cyber Security Program Review (Section A.4.3 of Appendix A to RG 5.71)*

*Section 4.3 of the VEGP CSP states that the applicant has established the necessary measures and governing procedures to implement periodic reviews of applicable program elements, in accordance with the requirements of 10 CFR 73.55(m). Specifically, the VEGP CSP calls for a review of the program's effectiveness at least every 24 months. In addition, reviews are to be conducted as follows:*

- *within 12 months following initial implementation of the program*
- *as necessary, based upon site-specific analyses, assessments, or other performance indicators*
- *as soon as reasonably practical, but no longer than 12 months after changes occur in personnel, procedures, equipment, or facilities that potentially could adversely affect cyber security*
- *by individuals independent of those personnel responsible for program management, and any individual who has direct responsibility for implementing the program*

*This deviates from RG 5.71 in the specific wording, but includes the same commitments. Specifically, RG 5.71 states that the licensee reviews the program's effectiveness at least every 24 months. In addition, reviews are conducted as follows:*

- *within 12 months of the initial implementation of the program*
- *within 12 months of a change to personnel, procedures, equipment, or facilities that potentially could adversely affect security*
- *as necessary based upon site-specific analyses, assessments, or other performance indicators*
- *by individuals independent of those personnel responsible for program implementation and management*

*Based on the above review, the NRC staff finds that the cyber security program review described in Section 4.3 of the VEGP CSP is acceptable.*

*13.8.4.23 <u>Document Control and Records Retention and Handling (Section A.5 of Appendix A to RG 5.71)</u>*

*Section 5 of the VEGP CSP states the necessary measures and governing procedures to ensure that sufficient records of items and activities affecting cyber security are developed, reviewed, approved, issued, used, and revised to reflect completed work. VEGP will retain records and supporting technical documentation required to satisfy the requirements of 10 CFR 73.54 and 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage," until the NRC terminates the facility's operating license. Records are retained to document access history, as well as to discover the source of cyber attacks or other security-related incidents affecting CDAs or SSEP functions, or both. VEGP Units 3 and 4 will retain superseded portions of these records for at least three years after the record is superseded, unless otherwise specified by the NRC.*

*This deviates from RG 5.71 by not specifically detailing the types of records, but instead describes that records will be retained to document access history and information needed to discover the source of cyber attacks and incidents. This is consistent with what is included in RG 5.71, Section 5, and includes all the performance-based characteristics and commitments of that section.*

*Based on the above review, the NRC staff finds that the document control and records retention handling described in Section 5 of the VEGP CSP is acceptable.*

*13.8.4.24 Deviations Taken to RG 5.71, Sections C.1 Through C.5*

*The VEGP CSP states that the plan deviates from Regulatory Positions C.1 through C.5 of RG 5.71, as noted in Attachment A to the CSP. For that reason, the staff considers that the full evaluation of the CSP must include a review of the deviations taken to those sections of RG 5.71 as listed in the VEGP CSP. This section of the SER lists those 68 specific deviations and their evaluated security impact. The following deviations were provided in a table, as part of Attachment A to the CSP.*

*13.8.4.24.1 RG 5.71, Section C.2, fourth paragraph, first sentence (page 8)*

*SNC added the term "adequately" to the phrase "…systems and equipment are protected from cyber attack." Since 10 CFR 73.54 specifically makes that same statement, the staff found no reason to object to that clarification. The objective is to provide adequate protection to the identified CDAs.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.2 RG 5.71, Section C.2, fourth paragraph, twelfth bullet, third sub-bullet (page 8)*

*SNC clarifies that its overall design is based on the Westinghouse AP1000 design and states that the AP1000 DCD commits to Revision 1 of RG 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." Since the applicant is required to have a cyber security program that meets the performance objectives outlined in 10 CFR 73.54 and is not obliged to achieve that requirement exclusively through the example provided by RG 5.71, this clarification, in and of itself, was not considered by the staff as deviating from the requirements established by the rule.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.3 RG 5.71, Section C.2, fifteenth bullet (page 8)*

*The deviation states that the required policies and procedures have not yet been written, reviewed, and approved, and, thus, are not currently available for inspection and review.*

*The NRC requires that these policies and procedures be completed and available for review by the completion of the CSP implementation schedule proposed by the applicant, since CSP inspections would not occur until that time. The requirements of 10 CFR 73.55(a)(4) and proposed License Condition 6 provide the necessary controls associated with developing the required policies and procedures of the CSP.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.4 RG 5.71, Section C.3, Figure 1 (Page 10)*

*The deviation changes the arrows on the left side of Figure 1 from "Continuous Monitoring" to "Ongoing Monitoring."*

*The NRC intended monitoring to occur periodically, and when required, based on certain inputs into the process. SNC states that "continuous" might imply that monitoring was perpetual and not event driven. This was not the staff's intent with the term "continuous." The staff accepts the use of the term "ongoing" to better reflect the intent of this diagram.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.5 RG 5.71, Section C.3, third paragraph, first sentence (Page 10)*

*The VEGP CSP changes the statement, "An acceptable method to establish a cyber security program at a facility is by performing the following, (1) analyze the digital computer and communication systems and networks, …" to "An acceptable method to establish a cyber security program at a facility is by performing the following: (1) identify critical systems and critical digital assets as described in Section C.3.1.3, (2) analyze the digital computer and communication systems and networks..."*

*This deviation is acceptable because SNC proposes to use its licensing basis to identify CSs that are associated with SSEP functions, as 10 CFR 73.54 requires. This statement includes the first step in RG 5.71 to analyze digital computer and communication systems and networks to determine if they include CDAs.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.6 RG 5.71, Section C.3.1, first paragraph, first sentence (page 11)*

*The VEGP CSP changes the statement, "Consistent with the requirements of 10 CFR 73.54(b)(1), a licensee must conduct a site-specific analysis of digital computer and communication systems and networks to identify CDAs, which are those assets that, if compromised, could adversely impact the SSEP functions of nuclear facilities." to "Consistent with the requirements of 10 CFR 73.54(b)(1), a licensee must conduct a site-specific analysis of digital computer and communication systems and networks to identify CDAs, which are those assets that, if compromised, could adversely impact the CSs of nuclear facilities."*

*SNC defines a CS as:*

> *An analog or digital technology-based system in or outside of the plant that performs or is associated with a safety-related, important-to-safety, security, or emergency preparedness function. These critical systems include, but are not limited to, plant systems, equipment, communication systems, networks, offsite communications, or support systems or equipment, that perform or are associated with a safety-related, important-to-safety, security, or emergency preparedness function as defined by the approved plant licensing basis.*

*This definition ties CSs to SSEP functions; therefore, the change is consistent with the method used in RG 5.71, as this means that CSs are all those assets associated with SSEP functions, and, therefore, could adversely impact those SSEP functions.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.7 RG 5.71, Section C.3.1, first paragraph, second bullet (page 11)*

*The VEGP CSP includes a deviation to correct an editorial omission in RG 5.71. Page 11 of RG 5.71 states that:*

*An acceptable method for identifying and documenting CDAs is as follows:*

- *obtain authorization for security assessment*
- *define roles and responsibilities cyber personnel and form the cyber security team*
- *identify and document CDAs at the facility*
- *review and validate configurations of CDAs*

*The VEGP CSP corrects the second bullet to read:*

- *define roles and responsibilities of cyber personnel and form the cyber security team*

*This deviation which supplies the omitted "of" is consistent with the intent of the referenced bullet.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.8 RG 5.71, Section C.3.1.2, third paragraph, second bullet (page 13)*

*The VEGP CSP changes the second bullet on Page 13 of RG 5.71 from:*

> *documenting all key observations, analyses, and findings during the assessment process so that this information can be used as a basis for applying security controls;*

*to:*

> *documenting all key observations, analyses, and findings during the assessment process so that this information can be used as a basis for addressing security controls;*

*This deviation is acceptable because RG 5.71 allows a licensee to address, as opposed to apply, security controls if it follows the process in Appendix A, Section 3.1.6 of RG 5.71, which is to apply the control, apply an alternative that provides no less protection than the corresponding security control, or to demonstrate that the control is not necessary because the attack vector, root cause, or vulnerability associated with the control does not exist.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.9 RG 5.71, Section C.3.1.2, third paragraph, sixth bullet (page 13)*

*The VEGP CSP changes the sixth bullet on Page 13 from:*

- *preparing documentation and overseeing implementation of the cyber security controls provided in Appendices B and C to this guide, documenting the basis for not implementing certain cyber security controls provided in Appendix B, or documenting the basis for the implementation of alternate or compensating measures in lieu of any cyber security controls provided in Appendix B; and*

*to:*

- *overseeing documentation and implementation of the cyber security controls provided in Appendices B and C to this guide, documenting the basis for not implementing certain cyber security controls provided in Appendix B and C, or documenting the basis for the implementation of alternate or compensating measures in lieu of any cyber security controls provided in Appendix B and C; and*

*This deviation is acceptable because overseeing the documentation and implementation of security controls by qualified personnel is an approved method. Further, the extension of this method in Appendix C is also acceptable*

*as the licensee has committed to follow the process in Appendix A, Section 3.1.6 of RG 5.71.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.10 RG 5.71, Section C.3.1.2, third paragraph, seventh bullet (page 13)*

*The VEGP CSP includes a deviation from RG 5.71 that changes bullet 7 from:*

> *assuring the retention of all assessment documentation, including notes and supporting information, in accordance with 10 CFR 73.54(h) and the record retention and handling requirements specified in Section C.5 of this guide.*

*to:*

> *establishing the retention policy of all assessment documentation, including notes and supporting information, in accordance with 10 CFR 73.54(h) and the record retention and handling requirements specified in Section C.5 of this guide.*

*This deviation is acceptable as the licensee has committed to establish the retention policy. Although this may be done by a different team, and not the CST, it is consistent with the intent of RG 5.71.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.11 RG 5.71, Section C.3.1.2, fourth paragraph, first sentence (page 13)*

*The VEGP CSP deviates from RG 5.71 by changing this sentence:*

> *The licensee's CST needs to have the authority to conduct an objective assessment, make determinations that are not constrained by operational goals (e.g., cost),*

*to:*

> *The licensee's CST needs to have the authority to conduct an objective assessment, make determinations that are not constrained by business goals (e.g., cost),*

*This deviation is acceptable because the intent of this statement in RG 5.71 is to ensure that cost is not used as a factor in making determinations about the*

*adequacy of security controls, vulnerabilities, identifying CSs and CDAs, and carrying out other assessment functions of the CST.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.12 RG 5.71, Section C.3.1.3, second paragraph (page 14)*

*The VEGP CSP deviates from RG 5.71 by changing the identification process from CDAs to CSs. This deviation is acceptable because the VEGP CSP commits to continue identifying CSs by identifying digital computers, networks, communication systems and support systems that perform and are associated with SSEP functions, as well as support systems and equipment that, if compromised, would adversely impact the plant's SSEP functions.*

*This is consistent with the process in RG 5.71, which identifies CDAs through the same process. The licensee further describes CDAs as a CS or part of a CS; therefore, the use of the term CS as opposed to CDA is also consistent with the method used in RG 5.71.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.13 RG 5.71, Section C.3.1.3, fifth paragraph, first sentence (page 15)*

*The VEGP CSP deviates from RG 5.71 by making an editorial correction to RG 5.71. This involves changing:*

> *With the identification of the all the CSs ...*

*to:*

> *With the identification of all the CSs ...*

*This change is acceptable because it accomplishes the intent of this phrase in RG 5.71 eliminating the unnecessary "the."*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.14 RG 5.71, Section C.3.1.3, fifth paragraph, second sentence (page 15)*

*The VEGP CSP deviates from RG 5.71 by changing the following statement from:*

> *A CDA may be a component of a CS ...*

*to:*

> *A CDA may be a complete CS or component of a CS, ...*

*This deviation is acceptable because this statement is factually true. A CDA may be a complete CS and the deviation does not change the level of protection provided by the method outlined in RG 5.71.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.15 RG 5.71, Section C.3.1.3, fifth paragraph, fifth sentence (page 15)*

*The VEGP CSP deviates from RG 5.71 by including additional documentation to help identify CSs and CDAs. Specifically VEGP includes "other licensing basis" documents to identify CSs and CDAs.*

*This deviation is in line with the intent of using existing documentation to identify CSs and CDAs. This section of RG 5.71 describes "helpful information sources for identifying CSs and CDAs" and is not an exhaustive list, nor is it the only method SNC has committed to use to identify CSs and CDAs. Specifically, SNC has committed to identify all digital computers, networks and communication systems associated with SSEP functions, which is what 10 CFR 73.54 requires.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.16 RG 5.71, Section C.3.1.3, eighth paragraph, first bullet (page 16)*

*The VEGP CSP deviates from RG 5.71 by stating that CDAs may be an entire CS. As previously discussed in Section 13.8.4.24.14 of this SER, it is true that a CDA may be an entire CS; therefore, this definition does not adversely impact either the method used in RG 5.71 or the protection that RG 5.71 provides.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.17 RG 5.71, Section C.3.1.3, eighth paragraph, second bullet (page 16)*

*The VEGP CSP deviates from RG 5.71 by stating that CDAs may be an entire CS. As previously discussed in Sections 13.8.4.24.14 and 13.8.4.24.16 of this SER, it is true that a CDA may be an entire CS; therefore, this definition does not adversely impact either the method used in RG 5.71 or the protection that RG 5.71 provides.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.18 RG 5.71, Section C.3.2, first paragraph, first sentence (page 18)*

*The VEGP CSP deviates from RG 5.71 by providing an editorial correction to RG 5.71. Specifically, the VEGP CSP changes the following sentence from:*

> *As stated in 10 CFR 73.54(c)(2), the licensee must design its cyber security program to apply and maintain integrate defense-in-depth protective strategies to ensure the capability to detect, prevent, respond to, mitigate, and recover from cyber attacks.*

*to:*

> *As stated in 10 CFR 73.54(c)(2), the licensee must design its cyber security program to apply and maintain integrated defense-in-depth protective strategies to ensure the capability to detect, prevent, respond to, mitigate, and recover from cyber attacks.*

*This deviation captures the intent of this sentence in RG 5.71 by correcting "integrate" to "integrated."*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.19 RG 5.71, Section C.3.2, second paragraph, fourth sentence (page 18)*

*The VEGP CSP deviates from RG 5.71 by pointing to an editorial error in RG 5.71. Specifically, the VEGP CSP changes the following sentence from:*

> *Therefore, defense-in-depth is achieved not only by implementing multiple security boundaries, but also by instituting and maintaining a robust program of security controls that assess,*

*protect, respond, prevent, detect, and mitigates an attack on a CDA and with recovery.*

*to:*

*Therefore, defense-in-depth is achieved not only by implementing multiple security boundaries, but also by instituting and maintaining a robust program of security controls that assess, protect, respond, prevent, detect, and mitigate an attack on a CDA and with recovery.*

*This deviation captures the intent of this sentence in RG 5.71 by correcting "mitigates" to "mitigate." Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.20 RG 5.71, Section C.3.2, third paragraph, first sentence (page 18)*

*The VEGP CSP deviates from RG 5.71 by pointing to an editorial error in RG 5.71. Specifically, the VEGP CSP changes the following sentence from:*

*For example, if a failure in prevention were to occur (e.g., a violation of policy) or if protection mechanisms were to be bypassed (e.g., by a new virus that is not yet identified as a cyber attack), mechanisms would still in place to detect and respond to an unauthorized alteration in an impacted CDA, mitigate the impacts of this alteration, and recover normal operations of the impacted CDA before an adverse impact.*

*to:*

*For example, if a failure in prevention were to occur (e.g., a violation of policy) or if protection mechanisms were to be bypassed (e.g., by a new virus that is not yet identified as a cyber attack), mechanisms would still be in place to detect and respond to an unauthorized alteration in an impacted CDA, mitigate the impacts of this alteration, and recover normal operations of the impacted CDA before an adverse impact.*

*This is acceptable because the change to add the word "be" to the phrase "would still be in place to detect" captures the intent of this sentence by supplying the "be" omitted from RG 5.71.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.21 RG 5.71, Section C.3.2.1, Figure 5 (Page 19)*

*The VEGP CSP includes a defensive architecture, which deviates from the example provided in RG 5.71. The proposed architecture is acceptable because it provides defense-in-depth, communication isolation for safety and security systems, and multiple nondeterministic boundaries for nonsafety/nonsecurity CDAs. This provides adequate protection for CDAs and ensures that appropriate isolation and boundary protection exists for all CDAs where appropriate.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.22 RG 5.71, Section C.3.2.1, third paragraph (page 19)*

*The VEGP CSP deviates from RG 5.71 by modifying the characteristics of an acceptable defensive architecture by stating that the architecture includes CSs and CDAs configured in accordance with Section 5 of Appendix B, and Sections 6 and 7 of Appendix C in accordance with the security control application process described in Section 3.3. As previously discussed in Section 13.8.4.24.9 of this SER, the use of the security control application process to address controls is consistent with RG 5.71.*

*SNC has committed to apply the security control, demonstrate that alternative controls provide no less protection than the corresponding control, or demonstrate through analysis that the attack vector the control addresses does not exist; therefore, the control is not necessary.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.23 RG 5.71, Section C.3.2.1, third paragraph, first bullet (page 19)*

*The VEGP CSP deviates from RG 5.71 by modifying the example defensive architecture to match the architecture to be used in the AP1000. This deviation is acceptable because it provides the appropriate isolation of safety and security CDAs, and adequate boundaries for nonsafety/nonsecurity CDAs.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.24 RG 5.71, Section C.3.2.1, third paragraph, second bullet (page 19)*

*The VEGP CSP deviates from RG 5.71 by modifying the example defensive architecture to match the architecture to be used in the AP1000. As previously discussed in Section 13.8.4.6, this deviation is acceptable because it provides the appropriate isolation of safety and security CDAs, and adequate boundaries for nonsafety/nonsecurity CDAs. This is consistent with the defensive model in*

*RG 5.71, as the VEGP defensive architecture provides boundaries for safety systems that are deterministic.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.25 RG 5.71, Section C.3.2.1, third paragraph, third bullet (page 19)*

*The VEGP CSP deviates from RG 5.71 regarding communications from digital assets at lower security levels to digital assets at higher security levels. This deviation is acceptable because the defensive architecture prevents specific communication from lower security levels to specific higher security levels. This is consistent with the defensive model in RG 5.71.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.26 RG 5.71, Section C.3.2.1, third paragraph, new second bullet (page 19)*

*The VEGP CSP deviates from RG 5.71 regarding remote access. This is consistent with the requirement in Section C.7 of RG 5.71, which also requires that remote access to CDAs at the highest level be prevented.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.27 RG 5.71, Section C.3.2.1, third paragraph, new sixth bullet (page 19)*

*The VEGP CSP deviates from RG 5.71 by including in its defensive architecture a statement from Section C.7 of RG 5.71 for validating data (software updates, new firmware, etc.) using a method at or above the level of security the CDA that will have data transferred to it. This concept is already acceptable in RG 5.71 and is also included in the defensive architecture, although in a different section of the document. This is consistent with the method used in RG 5.71 and does not adversely impact the protection provided.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.28 RG 5.71, Section C.3.2.1, third paragraph, seventh bullet (page 19)*

*The VEGP CSP deviates from RG 5.71 by changing the commitment to eliminate applications, services and protocols not necessary to support the design-basis function of the CDAs to eliminate, disable, or render these inoperable. This is consistent with the method in RG 5.71, because in some cases these elements*

*cannot be eliminated, but rather may have to be disabled or otherwise rendered inoperable. In each case, the result is the same. The asset is only configured to perform its design-based function and nothing more, which produces no less protection than the method in RG 5.71.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.29 RG 5.71, Section C.3.2.1, third paragraph, eighth bullet (page 19)*

*The VEGP CSP deviates from RG 5.71 by eliminating the requirement to configure CDAs and boundary protection systems in accordance with Section 5 of Section B and Sections 6 and 7 of Appendix C. However, the VEGP CSP does commit to this in the preamble statement as described in Section 13.8.4.24.22 of this SER. Therefore, the VEGP CSP provides the same commitment to perform this as does RG 5.71, albeit in a different part of the same section.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.30 RG 5.71, Section C.3.2.1, fourth paragraph (page 19)*

*The VEGP CSP deviates from RG 5.71 by deleting the paragraph that commits to applying the security controls. However, the VEGP security plan commits, in Section 3.1.6 of Appendix A, to address these controls and is, therefore, consistent with the method used in RG 5.71. The deleted paragraph is, therefore, unnecessary in the VEGP CSP to achieve the same commitment.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.31 RG 5.71, Section C.3.2.1, Prior to fifth paragraph (page 19)*

*The VEGP CSP deviates from the RG 5.71 defensive architecture. The VEGP architecture is described in Section 13.8.4.6 of this SER.*

*Based on the review and assessment in Section 13.8.4.6, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.32 RG 5.71, Section C.3.3, first paragraph, second sentence (page 20)*

*The VEGP CSP deviates from RG 5.71 by changing the following sentence:*

> *A cyber compromise of CDAs would adversely impact nuclear facilities' SSEP functions that are necessary for protecting public health and safety.*

*to:*

> *A cyber compromise of CDAs could adversely impact nuclear facilities' SSEP functions that are necessary for protecting public health and safety.*

*This deviation is consistent with the intent of RG 5.71, which implies that a compromise could lead to adverse impact and possible radiological sabotage. The intent of the paragraph is to establish the impact that could occur if a CDA were compromised. The security controls are designed around worst case scenarios, and the change in the VEGP CSP from "would" to "could" maintains this logic.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.33 RG 5.71, Section C.3.3, third paragraph, fourth sentence (page 20)*

*The VEGP CSP deviates from RG 5.71 by making an editorial correction to RG 5.71. This involves changing the statement:*

> *Thus to provide high assurance that CDAs are protected from cyber attacks, potential cyber risks of these CDAs must be addressed known potential cyber risks.*

*to:*

> *Thus to provide high assurance that CDAs are protected from cyber attacks, potential cyber risks of these CDAs must be addressed for known potential cyber risks.*

*This is acceptable because the change captures the intent of this sentence by supplying the "for" omitted from RG 5.71.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.34 RG 5.71, Section C.3.3, third paragraph, first sentence (page 20)*

*The VEGP CSP deviates from RG 5.71 by adding Appendix C to the list of controls that may be addressed using the method in Section 3.1.6 of Appendix A. This is consistent with the intent of RG 5.71, which assumes that all the controls in Appendix C can be implemented as written. However, if the controls can be addressed to demonstrate that an alternative control provides no less protection than the comparable control in Appendix C, or that the control is not necessary by demonstrating that the attack vector does not exist, this would meet the intent of RG 5.71.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.35 RG 5.71, Section C.3.3, third paragraph, first bullet (page 20)*

*The VEGP CSP deviates from RG 5.71 by adding Appendix C to the list of controls that may be addressed using the method in Section 3.1.6 of Appendix A. This is consistent with the intent of RG 5.71, which assumes that all the controls in Appendix C can be implemented as written. However, if the controls can be addressed to demonstrate that an alternative control provides no less protection than the comparable control in Appendix C, or that the control is not necessary by demonstrating that the attack vector does not exist, this would meet the intent of RG 5.71.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.36 RG 5.71, Section C.3.3, third paragraph, second bullet (page 20)*

*The VEGP CSP deviates from RG 5.71 by stating that alternative controls will not provide equal or better protection to the corresponding control, but rather that they will not provide less protection than the corresponding control. This is consistent with the method used in RG 5.71; providing an alternative that does not provide less protection, and does not adversely impact the security program. Therefore, this change in commitment will provide an adequate level of protection and is consistent with the method used in RG 5.71.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.37 RG 5.71, Section C.3.3, third paragraph, second bullet, second sub-bullet (page 20)*

*The VEGP CSP deviates from RG 5.71 by changing the statement:*

> *performing and documenting the attack vector and attack tree analyses of the CDA and alternative countermeasures to confirm that the countermeasures provide the same or greater protection as the corresponding security control in Appendix B.*

*to:*

> *performing and documenting an attack vector and attack tree analysis of the CDA and alternative countermeasures to confirm countermeasures provide no decrease in the effectiveness of protection as compared to the corresponding security control identified in Appendix B or C.*

*This deviation is acceptable because whether the licensee performs a single analysis or multiple analyses, the method is comparable provided that it will demonstrate that there is no decrease in protection. Further, the modification of the second part of the sentence is also acceptable because the intent of this method in RG 5.71 is to ensure that alternative controls do not provide less protection than the corresponding control. Therefore, a commitment to ensure that alternatives do not provide less protection produces a comparable level of protection as stating that the alternatives provide equal or better protection. Finally, the addition of the Appendix C controls to this method is acceptable because the licensee has committed to apply the control, apply an alternative that provides no less protection than the comparable control or not to apply the control and demonstrate that the attack vector does not exist.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.38 RG 5.71, Section C.3.3, third paragraph, second bullet, third sub-bullet (page 20)*

*The VEGP CSP deviates from RG 5.71 in a similar manner to deviations in Section 13.8.4.28.37 of this SER by changing the commitment to implement alternative countermeasures that provide at least the same degree of protection as the corresponding security control in Appendix B, to implementing alternative controls to provide no decrease in the effectiveness of protection as compared to the corresponding security control identified in Appendices B and C of RG 5.71.*

*This method is consistent with the method in RG 5.71 as it also meets the criteria for the performance based characteristics of 10 CFR 73.54. As long as the implemented alternative control does not provide less protection than the*

*corresponding control in RG 5.71, the intent of this section of RG 5.71 has been met. Alternative controls are considered to be adequate only if they provide equivalent protection, and the VEGP CSP commits to that minimum standard.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.39 RG 5.71, Section C.3.3, third paragraph, third bullet (page 20)*

*The VEGP CSP deviates from RG 5.71 by not stating that SNC will specifically perform an attack vector and attack tree analysis to demonstrate that one of the specific security controls is not necessary. SNC does commit to performing an analysis to demonstrate that the attack vector does not exist (i.e., is not applicable), thereby obviating the need for a specific security control.*

*This method is consistent with the method in RG 5.71 as it commits to demonstrating a conclusion, specifically, that the attack vector does not exist. If the licensee can demonstrate this, and not use an attack vector or attack tree analysis, the results are still the same and, therefore, the method would produce a result that does not provide less protection than the method in RG 5.71.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.40 RG 5.71, Section C.3.3, fourth paragraph, second sentence (page 20)*

*The VEGP CSP deviates from RG 5.71 by making an editorial correction to RG 5.71. This involves changing the statement:*

> *When a security control is determined to have an adverse affect, alternate controls should be used by the licensee to protect the CDA from cyber attack up to and including the DBT consistent with the process described above.*

*to:*

> *When a security control is determined to have an adverse effect, alternate controls should be used by the licensee to protect the CDA from cyber attack up to and including the DBT consistent with the process described above.*

*This is acceptable because the change captures the intent of this sentence in RG 5.71, by correcting "affect" to "effect."*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.41 RG 5.71, Section C.3.3, fifth paragraph, second sentence (page 21)*

*The VEGP CSP deviates from RG 5.71 by making an editorial correction to RG 5.71. This involves changing the statement:*

> *If these effectiveness or vulnerability analyses identify a gap in the cyber security program, the licensee may need to implement additional security measures and controls not provided in Appendixes B and C.*

*to:*

> *If these effectiveness or vulnerability analyses identify a gap in the cyber security program, the licensee may need to implement additional security measures and controls not provided in Appendices B and C.*

*This change is acceptable because it captures the intent of this sentence in RG 5.71, by correcting "Appendixes" to "Appendices."*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.42 RG 5.71, Sections C.3.3.1.1 through C.3.3.1.5, first paragraph and last bullet (pages 21 and 22)*

*The VEGP CSP deviates from RG 5.71 by stating that it will not apply all of the security controls in RG 5.71, but rather will address them. The VEGP CSP already commits to the RG 5.71 process, which is:*

1) *applying controls;*

2) *applying an alternative control that does not provide less protection than the corresponding control; or*

3) *not applying a control, but demonstrating that the corresponding attack vector does not exist.*

*The intent of RG 5.71 is to address the controls in Appendices B and C. This can be accomplished in accordance with Section 3.1.6 of Appendix A, to which SNC has committed.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.43 RG 5.71, Section C.3.3.1.1, first paragraph, second bullet, fourth sub-bullet (page 21)*

*The VEGP CSP deviates from RG 5.71 by committing to audit CDAs at an interval defined for the CDA, or within 5 days following revocation of an individual's unescorted access, due to a lack of trustworthiness or reliability, or as soon as reasonably practical upon changes in personnel. Although this method uses a different frequency than the method in RG 5.71, which calls for annual assessments, or assessments immediately upon changes in personnel, this frequency does meet the requirements of 10 CFR 73.55(m), which allows the licensee to define these intervals based on its own assessments of need.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.44 RG 5.71, Sections C.3.3.2.1 through C.3.3.2.5, first paragraph and last bullet (pages 23 and 24)*

*The VEGP CSP deviates from RG 5.71 in a fashion similar to the deviation cited in Section 13.8.4.24.42 of this SER by committing not to apply the controls, but rather to address them. As previously stated, this deviation is consistent with the method in RG 5.71, and also meets the intent of the RG, provided that the licensee follows the process in Section 3.1.6 of Appendix A, to which SNC has committed.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.45 RG 5.71, Sections C.3.3.2.6 through C.3.3.2.9, first paragraph and last bullet (pages 24-26)*

*The VEGP CSP deviates from RG 5.71 in a fashion similar to the deviation cited in Sections 13.8.4.24.42 and 13.8.4.24.44 of this SER by committing to apply the controls, but rather to address them. As previously stated, this deviation is consistent with the method in RG 5.71, and also meets the intent of the RG, provided that the licensee follows the process in Section 3.1.6 of Appendix A, to which SNC has committed.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.46 RG 5.71, Section C.3.3.2.9, first paragraph, first bullet (page 25)*

*The VEGP CSP deviates from RG 5.71 by making an editorial correction to RG 5.71. This involves changing the first bullet:*

- *develop, disseminate, and annually review and update the configuration management policy and program which defines the purpose of the nuclear facility's configuration management policy, scope, roles, requirements, responsibilities, and management commitments necessary to provide, with high assurance, that (1) when a modification to a CDA does not reduce the existing security and (2) any unauthorized or inadvertent modification of a CDA is prevented.*

*to:*

- *develop, disseminate, and annually review and update the configuration management policy and program which defines the purpose of the nuclear facility's configuration management policy, scope, roles, requirements, responsibilities, and management commitments necessary to provide, with high assurance, that (1) a modification to a CDA does not reduce the existing security and (2) any unauthorized or inadvertent modification of a CDA is prevented.*

*This is acceptable because it captures the intent of this sentence in RG 5.71, by striking the word "when" after "(1)." This editorial mistake will be corrected in a future revision.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.47 RG 5.71, Section C.3.3.3.1, first paragraph and last bullet (page 26)*

*The VEGP CSP deviates from RG 5.71 in a fashion similar to the deviations cited in Sections 13.8.4.24.42, 13.8.4.24.44 and 13.8.4.24.45 of this SER, and by committing not to apply the controls, but rather to address them. As previously stated, this deviation is consistent with the method in RG 5.71, and also meets the intent of RG 5.71, provided that the licensee follows the process in Section 3.1.6 of Appendix A, to which SNC has committed.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.48 RG 5.71, Section C.3.3.3.1, second paragraph (page 26)*

*The VEGP CSP deviates from RG 5.71 by committing to Revision 1 of RG 1.152 and not Revision 2 of RG 1.152 as stated in RG 5.71. The results of the NRC staff's technical evaluation of the digital instrumentation and controls design of the AP 1000 are documented in Chapter 7 of NUREG-1793 and its supplements. SNC's use of the defensive architecture as discussed in Section 13.8.4.6 is acceptable to the staff.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.49 RG 5.71, Section C.3.3.3.2, first paragraph, second sentence (page 26)*

*The VEGP CSP deviates from RG 5.71 by committing to provide adequate protection of high assurance against cyber attacks. Although this commitment is worded differently than the commitment provided in RG 5.71, it does meet the requirement of 10 CFR 73.54(a), which states that licensees "shall 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."*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.50 RG 5.71, Section C.3.4, second paragraph, first sentence (page 26)*

*The VEGP CSP deviates from RG 5.71 as described in Section 13.8.4.8 of this SER by committing not to integrate management of physical and cyber security, but rather to provide the management interfaces necessary to appropriately coordinate the physical and cyber security activities. The VEGP CSP includes a commitment to establish an organization that is responsible for cyber security and is independent of operations. The combination of an independent organization responsible for cyber security, and management coordination between physical and cyber security meets the requirements of the rule and does not provide less protection than the method described in RG 5.71.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.51 RG 5.71, Section C.3.4, second paragraph, first bullet (page 27)*

*The VEGP CSP deviates from RG 5.71 as also described in Section 13.8.4.8 of this SER by committing not to form a unified security organization, but rather to establish a cyber security organization that is responsible for cyber security and is independent from operations. The combination of an independent organization responsible for cyber security, and management coordination as described in Section 13.8.4.24.51 of this SER between physical and cyber security meets the requirements of the rule, and does not provide less protection than the method described in RG 5.71.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.52 RG 5.71, Section C.4, first paragraph, first sentence (page 27)*

*The VEGP CSP deviates from RG 5.71 by changing the phrase:*

> *Once the security program is in place...*

*to:*

> *Once the cyber security program is in place...*

*This deviation is acceptable because the CSP only applies to the applicant's cyber security program.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.53 RG 5.71, Section C.4, first paragraph, first bullet (page 28)*

*The VEGP CSP deviates from RG 5.71 as previously described in Section 13.8.4.11 of this SER by changing the phrase "continuous monitoring and assessment" to "ongoing monitoring and assessment." This description is consistent with the method in RG 5.71 by establishing intervals for these assessments, which include the same elements as in RG 5.71, and meeting the periodicity requirements of 10 CFR 73.55(m).*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.54 RG 5.71, Section C.4.1, section heading and first paragraph, first sentence (page 28)*

*The VEGP CSP deviates from RG 5.71 as previously described in Sections 13.8.4.11 and 13.8.4.24.53 of this SER by changing the phrase "continuous monitoring and assessment" to "ongoing monitoring and assessment." This description is consistent with the method in RG 5.71 by establishing intervals for these assessments, which include the same elements in RG 5.71 and meeting the periodicity requirements of 10 CFR 73.55(m).*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.55 RG 5.71, Section C.4.1, second paragraph, first sentence (page 28)*

*The VEGP CSP deviates from RG 5.71 as previously described in Sections 13.8.4.11, 13.8.4.53 and 13.8.4.24.54 of this SER by changing the phrase "continuous monitoring and assessment" to "ongoing monitoring and*

*assessment." This description is consistent with the method in RG 5.71 by establishing intervals for these assessments, which include the same elements as in RG 5.71 and meeting the periodicity requirements of 10 CFR 73.55(m).*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.56 RG 5.71, Section C.4.1, second paragraph, first bullet (page 28)*

*The VEGP CSP deviates from RG 5.71 by making an editorial correction to RG 5.71. This involves changing the phrase:*

> *ongoing assessments of verify that the security controls...*

*to:*

> *ongoing assessments to verify that the security controls...*

*This change is acceptable because it captures the intent of this sentence in RG 5.71, by substituting "to" for "of."*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.57 RG 5.71, Section C.4.1, third paragraph, first and second sentences (page 28)*

*The VEGP CSP deviates from RG 5.71 as previously described in Sections 13.8.4.11, 13.8.4.53, 13.8.4.24.54 and 13.8.4.24.55 of this SER by changing the phrase "continuous monitoring and assessment" to "ongoing monitoring and assessment." This description is consistent with the method in RG 5.71 by establishing intervals for these assessments, which include the same elements as in RG 5.71, and meeting the periodicity requirements of 10 CFR 73.55(m).*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.58 RG 5.71, Section C.4.1.1, first paragraph, second sentence (page 28)*

*Section 3.1.1 of the VEGP CSP states that status of security controls will be verified in accordance with the requirements of 10 CFR 73.55(m).*

*The NRC staff reviewed the above and found that reviewing security controls in accordance with 10 CFR 73.55(m) is in accordance with RG 5.71. The time period between evaluations may be longer than the time period provided in*

*RG 5.71. However, this period cannot exceed 24 months, which conforms to 10 CFR 73.54(g), requiring the applicant to review the cyber security program as a component of the physical security program in accordance with the requirements of 10 CFR 73.55(m), including the periodicity requirements. The requirements of 10 CFR 73.55(m) are that, at minimum, the applicant review each element of the physical protection program at least every 24 months.*

*The licensee has also committed to address C.13 of Appendix C to RG 5.71, "Security Assessment and Risk Management," which calls for vulnerability assessments on a quarterly basis. SNC commits to apply this control, apply an alternative that provides no less protection than C.13, or demonstrate that any attack vectors associated with vulnerabilities that may be discovered through quarterly assessments do not exist. The VEGP CSP also includes addressing controls that specifically include defined verification periods and that detect when some controls are not working correctly.*

*This, coupled with the CSP conforming to requirements of 10 CFR 73.55(m), which includes an initial assessment within 12 months of the program inception, and as necessary based on site-specific analyses, assessments, or other performance indicators, provides a level of protection consistent with the method in RG 5.71.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.59 RG 5.71, Section C.4.1.2, first paragraph, third sentence (page 29)*

*Section 3.1.1 of the VEGP CSP states that effectiveness of security controls will be verified in accordance with the requirements of 10 CFR 73.55(m). As previously discussed in Section 13.8.4.12 of this SER, the NRC staff reviewed the above and found that the period of effectiveness analysis is comparable with that of RG 5.71.*

*The time period between evaluations is 12 months longer than the time period provided in RG 5.71. However, this 24-month time period conforms to 10 CFR 73.54(g) requiring the applicant to review the cyber security program as a component of the physical security program in accordance with the requirements of 10 CFR 73.55(m), including the periodicity requirements. The requirements of 10 CFR 73.55(m) are that, at minimum, the applicant review each element of the physical protection program, which includes the cyber security program, at least every 24 months and within 12 months of the implementation of the program, or within 12 months when changes that may adversely impact the security program occur.*

*Furthermore, the VEGP CSP states that controls will be reviewed according to the requirements of the security controls if that period of review occurs more often. This is also consistent with the method provided in RG 5.71.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.60 RG 5.71, Section C.4.1.3, first paragraph, second sentence (page 29)*

*VEGP CSP Section 4.1.3 deviates from RG 5.71 by stating that vulnerability assessments will occur periodically. RG 5.71, Section C.4.1.3 states that vulnerability assessments will occur no less frequently than on a quarterly basis.*

*As previously described in Section 13.8.4.14 of this SER, the VEGP CSP states vulnerability assessments will be performed as specified in the security controls in Appendices B and C of RG 5.71, and when new vulnerabilities that could affect the effectiveness of the cyber security program and the security of the CDAs are identified. The licensee also commits to addressing vulnerabilities that could cause CDAs to become compromised or could have an adverse impact on SSEP functions. Section 13.1 of Appendix C of RG 5.71, which VEGP commits to address in accordance with the process in Section 3.1.6 of Appendix A, provides that vulnerability assessments should occur no less frequently than once a quarter, at random intervals, and when new potential vulnerabilities are reported and identified. SNC has not deviated from the interval.*

*The process the applicant has committed to in Section 3.1.6 of the VEGP CSP requires SNC, if it does not implement Section 13.1 of Appendix C, to implement an alternate control that does not provide less protection than the corresponding control in Appendices B and C, or to demonstrate that any attack vectors associated with vulnerabilities that may be discovered through quarterly assessments do not exist.*

*Therefore, if SNC does not implement the security control in Appendix C, Section 13.1 of RG 5.71, or deviates from the guidance for a quarterly vulnerability assessment, it will ensure that this deviation does not provide less protection than performing quarterly vulnerability assessments, and will provide an analysis that demonstrates that the attack vector does not exist and will document this justification for inspection.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.61 RG 5.71, Section C.4.2, first paragraph, second sentence (page 30)*

*The VEGP CSP deviates from RG 5.71 by committing not to implement the security controls in Section 11 of Appendix C of RG 5.71, but rather to address those controls in accordance with Section C.3.3 of RG 5.71.*

*As previously described in Section 13.8.4.7 of this SER, the VEGP CSP deviates from RG 5.71 by committing to address security controls rather than committing to apply them. The VEGP CSP states that when a control from Appendices B and C of RG 5.71, such as Section 11 of Appendix C, is not implemented that the licensee will implement alternate control(s) that "do not provide less protection that the corresponding" control in the appendix. This deviation is consistent with the method used in RG 5.71, which states that controls should provide equal or better protection.*

*As also previously discussed in Section 13.8.4.7 of this SER, the VEGP CSP deviates from RG 5.71 by stating that when a control can be proven to be unnecessary, the applicant will perform an analysis demonstrating that the control is not necessary, and will provide a documented justification. Therefore, SNC commits that in addressing the security controls in Appendix C, Section 11 of RG 5.71 that it will either apply the control, apply an alternative that does not provide less protection or will demonstrate that the control is not necessary because the attack vectors do not exist. This method is consistent with the method used in RG 5.71, which also allows for controls to be addressed.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.62 RG 5.71, Section C.4.2.1, first paragraph, third sentence (page 30)*

*The VEGP CSP deviates from RG 5.71 in a manner similar to the previous deviation in Section 13.8.4.24.61 of this SER. Specifically, that configuration management will be used to ensure that each of the controls is addressed in Appendices B and C of RG 5.71, as opposed to implemented. This method is consistent with the method in RG 5.71, as the applicant commits to follow the process in Section C.3.3 of RG 5.71, which requires that the applicant implement the control, apply an alternative control that does not provide less protection than the corresponding control in RG 5.71, or demonstrate that the attack vector associated with the control does not exist. Therefore, the VEGP CSP method will provide no less protection than the method provided for in RG 5.71.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.63 RG 5.71, Section C.4.2.1, second paragraph, third sentence (page 30)*

*The VEGP CSP deviates from RG 5.71 by including the statement, "in accordance with the process described in Section C.3.3 of this guide." As previously discussed in Section 13.8.4.14 of this SER, the method in Section C.3.3 is consistent with the method in RG 5.71, which requires that the licensee either implement the control, apply an alternative control that does not*

*provide less protection than the corresponding control in RG 5.71, or demonstrate that the attack vector associated with the control does not exist. Therefore, the VEGP CSP method will provide no less protection than the method provided for in RG 5.71.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.64 RG 5.71, Section C.4.3, second paragraph (page 31)*

*The VEGP CSP deviates from RG 5.71, as previously discussed in Section 13.8.4.22 of this SER, by stating that the applicant has established the necessary measures and governing procedures to implement periodic reviews of applicable program elements, in accordance with the requirements of 10 CFR 73.55(m). Specifically, the VEGP CSP calls for a review of the program's effectiveness at least every 24 months. In addition, reviews are to be conducted as follows:*

- *within 12 months following initial implementation of the program*
- *as necessary based upon site-specific analyses, assessments, or other performance indicators*
- *as soon as reasonably practical, but no longer than 12 months, after changes occur in personnel, procedures, equipment, or facilities that potentially could adversely affect cyber security*
- *by individuals independent of those personnel responsible for program management and any individual who has direct responsibility for implementing the program*

*This deviates from RG 5.71 in the specific wording, but includes the same commitments as RG 5.71. Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.65 RG 5.71, Section C.5, second paragraph, second and third sentences (page 32)*

*As previously discussed in Section 13.8.4.23, the VEGP CSP deviates from RG 5.71 documentation retention commitments. Specifically, VEGP CSP Section 5 states the records are retained to document access history and information needed to discover the source of cyber attacks and incidents. The VEGP CSP deletes the phrase:*

> *Records required for retention include, but are not limited to, digital records, log files, audit files, and nondigital records that capture, record, and analyze network and CDA events.*

*The VEGP CSP commits to retaining all access history records, records to discover the source of cyber attacks or other security-related incidents affecting CDAs or SSEP functions, or both. This is consistent with what is included in RG 5.71 Section 5, as it includes all the performance-based characteristics and commitments of that section.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.66 RG 5.71, Glossary (Page 35)*

*The VEGP CSP's definition of a CDA deviates from the definition provided in RG 5.71. Specifically, the VEGP CSP deviates by stating that a CDA can be a CS or a subcomponent of a CS. This definition does not materially change the use of the term, and is correct: A CDA can be a CS. This definition is consistent with the definition in RG 5.71. The VEGP CSP, by the use of this definition, does not provide for less protection than RG 5.71, nor does this reduce the scope of the assets required to be protected under the rule.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.67 RG 5.71, Glossary (Page 35)*

*The VEGP CSP deviates from the definition of a CS in RG 5.71 by adding the caveat "as defined by the plant licensing basis." RG 5.71 states that a CS is an analog or digital technology based system in or outside the plant that performs or is associated with a safety-related, important-to-safety, security, or emergency preparedness function. These CSs include, but are not limited to, plant systems, equipment, communication systems, networks, offsite communications, or support systems or equipment, that perform or are associated with safety-related, important-to-safety, security, or emergency preparedness functions.*

*The addition of the phrase "as defined by the plants' licensing basis," limits the scope of the functions to those that are defined by the licensing basis. As previously discussed in Section 13.8.4.4 of this SER, the staff was concerned that this modifier might cause the licensee to exclude CSs, which ought to be included, according to the rule. 10 CFR 73.51(a)(1) requires that the licensee 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 SSEP functions. However, further reviews resulted in the staff finding that the VEGP CSP scoping discussion adequately described a process to include all CDAs within the scope of 10 CFR 73.54(a)(1).*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*13.8.4.24.68 RG 5.71, Glossary (Page 35)*

*The VEGP CSP deviates from the RG 5.71 definition of cyber attack by replacing the phrase "conducted by threat agents having either malicious or non-malicious intent" with the phrase "conducted by threat agents." The NRC staff finds this deviation to be acceptable because deletion of the intent of a threat agent, be it malicious or non-malicious, still provides a commitment to protect against threats by threat agents.*

*Based on the above review and assessment, the NRC staff finds that this deviation is acceptable.*

*License Conditions*

- *Part 10, License Condition 2, COL Item 13.6-5 and License Condition 3, Item G.10*

*The applicant proposed two license conditions in Part 10 of the VEGP COL application, which will require the applicant to implement the cyber security program prior to initial fuel load.*

*In a letter dated October 22, 2010, the applicant provided supplemental information which proposed to amend the milestone included in Part 2, FSAR Table 13.4-201 to implement the cyber security program prior to receipt of fuel onsite (protected area.) The NRC staff finds the proposed implementation milestone for the cyber security program (security prior to receipt of fuel onsite (protected area)) appropriate and in accordance with the requirement in 10 CFR 73.55. Therefore the staff finds that the proposed License Conditions 2 and 3 are not necessary.*

- *Part 10, License Condition 6*

*The applicant proposed a license condition in Part 10 of the VEGP COL application to provide a schedule to support the NRC's inspection of operational programs, including the cyber security program. Although the CSP is not identified as an operational program in SECY-05-0197, the proposed license condition is consistent with the policy established in SECY-05-0197 for operational programs in general, and is acceptable.*

VCSNS Clarifying Information Regarding License Condition 2, COL Item 13.6-5

VCSNS COL application, Part 10, Revision 2 did not include License Condition 2, COL Item 13.6-5 regarding CSP. Therefore, the discussion above regarding removal of this license condition is not applicable to VCSNS.

### 13.8.5 Post Combined License Activities

For the reasons discussed in the technical evaluation section above, the staff finds the following license condition proposed by the applicant acceptable:

- License Condition (13-7) - The licensee shall submit to the Director of NRO, a schedule, no later than 12 months after issuance of the COL, that supports planning for and conduct of NRC inspection of the operational programs listed in VCSNS COL FSAR Table 13.4-201, including the cyber security program implementation. The schedule shall be updated every 6 months until 12 months before scheduled fuel load, and every month thereafter until either the operational programs listed in VCSNS COL FSAR Table 13.4-201 have been fully implemented or the plant has been placed in commercial service, whichever comes first.

### 13.8.6 Conclusion

The NRC staff reviewed the application and checked the referenced DCD. The NRC staff's review confirmed that the applicant addressed the required information relating to cyber security, and there is no outstanding information expected to be addressed in the VCSNS COL FSAR related to this section. The results of the NRC staff's technical evaluation of the information incorporated by reference in the VCSNS COL application are documented in NUREG-1793 and its supplements.

The NRC staff has reviewed the CSP for format and content using the NRC CSP template in RG 5.71, and found it, pending closure of **Confirmatory Item 13.8-1**, to include all features considered essential to such a program. In particular the staff has found it to comply with applicable commission regulations including 10 CFR 73.1, 10 CFR 73.54, 10 CFR 73.55(a)(1), 10 CFR 73.55(b)(8), 10 CFR 73.55(m), and 10 CFR Part 73, Appendix G.