Safety Evaluation Report With Open Items for the U.S. EPR

Chapter 13, "Conduct of Operations"

CONTENTS

LIST OF FIGURES

No figures were included in this chapter.

LIST OF TABLES

13 CONDUCT OF OPERATIONS

U.S. EPR FSAR Chapter 13, "Conduct of Operations," provides information relating to the preparations and plans for design, construction, and operation of the U.S. EPR. U.S. EPR FSAR Chapter 13 provides adequate assurance that an applicant will establish and maintain a staff of adequate size and technical competence, and that operating plans are adequate to protect public health and safety. The scope of this chapter consists of the following areas:

- Organization
- Training
- Emergency Preparedness (EP)
- Operational Program Implementation
- Plant Procedures
- Security
- Fitness for Duty

13.1 Organizational Structure of Applicant

13.1.1 Introduction

Section 13.1, "Organizational Structure of Applicant," of the U.S. EPR Final Safety Analysis Report (FSAR) addresses structure, functions, and responsibilities of the management, technical support, and operating organizations established to operate and maintain the plant.

13.1.2 Summary of Application

FSAR Tier 1: There are no FSAR Tier 1 entries for this area of review.

FSAR Tier 2: The applicant has provided an FSAR Tier 2 program description in Section 13.1, summarized here, in part, as follows:

A combined license (COL) applicant that references the U.S. EPR design certification will provide site-specific information for management, technical support, and operating organizations. Additional information for a COL applicant to develop an operating organization is provided in Chapter 18, "Human Factors Engineering."

ITAAC: There are no inspections, tests, analyses, and acceptance criteria (ITAAC) items for this area of review.

Technical Specifications: The Technical Specifications (TS) associated with FSAR Tier 2, Section 13.1 are given in FSAR Tier 2, Chapter 16, Sections 5.1, "Responsibility," 5.2, "Organization," and 5.3, "Unit Staff Qualifications."

13.1.3 Regulatory Basis

The relevant requirements of Nuclear Regulatory Commission (NRC) regulations for this area of review, and the associated acceptance criteria, are given in NUREG-0800, Section 13.1, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," (hereafter referred to as NUREG-0800 or the SRP) and are summarized below. Review interfaces with other SRP sections can be found in NUREG-0800, Section 13.1.

1. Title 10 of the *Code of Federal Regulations* (10 CFR) 50.40(b), "Common Standards," as it relates to the requirements that the applicant be technically qualified to engage in activities associated with the design, construction, and operation of a nuclear power plant.

2. 10 CFR 50.54(j), (k), (l), and (m), "Conditions of Licenses," as they relate to the requirements for the presence of a licensed operator at the controls at all times during operation of the facility, for such operator's knowledge and consent to changes in reactivity or reactor power other than through the controls, for a licensed senior operator to direct the licensed activities of licensed operators, and for senior operator availability at the facility during reactor operations and other specific reactor conditions or modes of operation.

Acceptance criteria adequate to meet the above requirements include:

1. Regulatory Guide (RG) 1.8, "Qualification and Training of Personnel for Nuclear Power Plants"

2. NUREG-0711, "Human Factors Engineering Program Review Model"

3. NUREG-0737, "Clarification of TMI Action Plan Requirements"

13.1.4 Technical Evaluation

In FSAR Tier 2, Section 13.1, the applicant stated that a COL applicant referencing the U.S. EPR certified design will provide site-specific information for management, technical support, and operating organizations. This is COL Information Item 13.1-1. The staff also discusses its evaluation of the organizational structure of the applicant in Section 18.5 of this report. There are no areas where additional information needs to be provided in the design certification application.

13.1.5 Combined License Information Items

Table 13.1-1 provides a list of organizational structure of the applicant related COL information item numbers and descriptions from FSAR Tier 2, Table 1.8-2:

Table 13.1-1 U.S. EPR Combined License Information Items

Item No.	Description	FSAR Tier 2 Section
13.1-1	A COL applicant that references the U.S. EPR design certification will provide site-specific information for management, technical support, and operating organizations.	13.1

The staff finds the above listing to be complete. Also, the list adequately describes actions necessary for the COL applicant. No additional COL information items need to be included in FSAR Tier 2, Table 1.8-2 for identification of the organizational structure of the applicant.

13.1.6 Conclusions

The staff reviewed the application in accordance with the guidance provided in NUREG-0800, Sections 13.1.1, 13.1.2, 13.1.3, and the associated referenced NRC RGs. Based on its review of FSAR Tier 1, and FSAR Tier 2 Section 13.1 information, the staff concludes that a COL applicant referencing the U.S. EPR certified design will provide the required site-specific information for delineation of the management, technical support, and operating organizations in accordance with 10 CFR 50.40(b).

13.2 Training

13.2.1 Introduction

FSAR Tier 2, Section 13.2, "Training," addresses the description and schedule of the training program for licensed and non-licensed plant staff. The licensed operator training program also includes the requalification training program as required in 10 CFR 50.54(i-1), "Conditions of licenses," and 10 CFR 55.59, "Requalification."

13.2.2 Summary of Application

FSAR Tier 1: There are no FSAR Tier 1 entries for this area of review.

FSAR Tier 2: The applicant has provided a FSAR Tier 2 program description in Section 13.2, summarized here, in part, as follows:

A COL applicant that references the U.S. EPR design certification will provide site-specific information for training programs for plant personnel. Additional information for a COL applicant to develop training programs for plant personnel is provided in FSAR Tier 2, Chapter 18.

ITAAC: There are no ITAAC items for this area of review.

Technical Specifications: The Technical Specifications associated with FSAR Tier 2, Section 13.2, are provided in FSAR Tier 2, Chapter 16, Section 5.3.

13.2.3 Regulatory Basis

The relevant requirements of NRC regulations for this area of review and the associated acceptance criteria are listed in NUREG-0800, Sections 13.2.1 and 13.2.2 and are summarized below:

1. 10 CFR 50.54, “Conditions of Licenses,” Paragraphs (i-1), as it relates to the requirement to have in effect an operator requalification program that meets the requirements of 10 CFR 55.59(c).

2. 10 CFR 55.4, “Definitions,” as it relates to a detailed description of the training programs developed using a systems approach to training.

3. 10 CFR 55.31, “How to Apply,” as it relates to the content of applications for operators’ licenses.

4. 10 CFR 55.41, “Written Examination: Operators,” as it relates to the content of written examination for operators.

5. 10 CFR 55.43, “Written Examination: Senior Operators,” as it relates to the content of written examination for senior operators.

6. 10 CFR 55.45, “Operating Tests,” as it relates to the operating tests administered to applicants for operator and senior operator licenses.

7. 10 CFR 55.46, “Simulation Facilities,” as it relates to the use of simulation facilities for the administration of the operating test and plant-referenced simulators to meet experience requirements for applicants for operator and senior operator licenses.

8. 10 CFR 50.34(f)(2)(i), “Contents of Construction Permit and Operating License Applications; Technical Information,” as it relates to providing a simulator capability for the plant.

9. 10 CFR Part 50, Appendix E, Sections II.F and IV.F, “Emergency Planning and Preparedness For Production and Utilization Facilities,” as it relates to training and exercises for emergency radiation plans.

10. 10 CFR 50.120, “Training and Qualification of Nuclear Power Plant Personnel,” as it relates to positions to be covered by training programs.

Review interfaces with other SRP sections also can be found in NUREG-0800, Sections 13.2.1 and 13.2.2.

Acceptance criteria adequate to meet the above requirements include:

1. RG 1.8, “Qualification and Training of Personnel for Nuclear Power Plants”

2. RG 1.49, “Nuclear Power Plant Simulation Facilities for Use in Operator Training and License Examinations”

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

4. NUREG-1021, “Operator Licensing Examination Standards for Power Reactors”

5. NUREG-1220, “Training Review Criteria and Procedures”

6. SECY 05-0197, “Review of Operation Programs in a Combined License Application and Generic Emergency Planning Inspections, Tests, Analyses, and Acceptance Criteria [ITAAC]”

13.2.4 Technical Evaluation

In FSAR Tier 2, Section 13.2, “Training,” the applicant stated that a COL applicant referencing the U.S. EPR certified design will provide site-specific information for training programs for plant personnel. This is COL Information Item 13.2-1. The staff also discusses its evaluation of training in Section 18.9 of this report. There are no areas where additional information needs to be provided in the design certification application.

13.2.5 Combined License Information Items

Table 13.2-1 provides a list of training related COL information item numbers and descriptions from FSAR Tier 2, Table 1.8-2:

Table 13.2-1 U.S. EPR Combined License Information Items

Item No.	Description	FSAR Tier 2 Section
13.2-1	A COL applicant that references the U.S. EPR design certification will provide site-specific information for training programs for plant personnel.	13.2

The staff determined the above listing to be complete. Also, the list adequately describes actions necessary for the COL applicant. No additional COL information items need to be included in FSAR Tier 2, Table 1.8-2 for training consideration.

13.2.6 Conclusions

In FSAR Tier 2, Section 13.2, the applicant stated that a COL applicant referencing the U.S. EPR certified design will provide site-specific information on training programs for plant personnel. The training program is not within the scope of the U.S. EPR design certification and will be provided on a site-specific basis by each COL applicant referencing the U.S. EPR design. The staff will review the training program in the context of each COL application, and this is acceptable.

13.3 Emergency Planning

13.3.1 Introduction

Non-site-specific facilities, functions, and equipment which are technically relevant to the design and which affect some aspect of emergency planning or the capability of a COL applicant to cope with plant emergencies are described in this section. Emergency planning is, in large measure, within the scope of a COL applicant. A COL applicant that references the U.S. EPR design certification will provide a site-specific emergency plan in accordance with 10 CFR 50.47, "Emergency Plans," and 10 CFR Part 50, Appendix E, "Emergency Planning and Preparedness for Production and Utilization Facilities."

13.3.2 Summary of Application

FSAR Tier 1: There are no FSAR Tier 1 entries for this area of review.

FSAR Tier 2: The applicant has provided an FSAR Tier 2 system description in Section 13.3, "Emergency Planning," summarized here, in part, as follows:

The FSAR states that space suitable for a technical support center (TSC) is provided within the Safeguard Building, which is within the control room envelope (CRE), so that habitability during normal, off-normal, and emergency conditions can be maintained.

Data communications within the TSC are to be provided through the process information and control system which allows plant parameter monitoring during normal, off-normal, and emergency conditions.

The FSAR states that space suitable for an operational support center (OSC) is provided in the Access Building. The Access Building will also contain a personnel decontamination area.

Voice communications among the TSC; OSC; plant, local and offsite emergency response facilities; local and State governments; and NRC are to be provided by plant telephone, paging, and radio systems.

ITAAC: There are no ITAAC items for this area of review.

U.S. EPR Plant Interfaces: This section of the FSAR contains information related to the following plant interfaces that will be addressed in the COL designs: See FSAR Tier 2, Table 1.8-1, "Summary of U.S. EPR Plant Interfaces with Remainder of Plant," Item 13.2, "Site-specific emergency plan."

13.3.3 Regulatory Basis

The relevant requirements of NRC regulations for this area of review, and the associated acceptance criteria, are given in NUREG-0800, Section 13.3 and are summarized below. Review interfaces with other SRP sections also can be found in NUREG-0800, Section 13.3.

1. 10 CFR 50.47(b) including 10 CFR 50.47(b)(8) as it relates to providing adequate facilities to accommodate emergency response staff, 10 CFR 50.47(b)(9) as it relates to systems and equipment to assess and monitor actual or potential accident

consequences, and (b)(11) as it relates to means for controlling exposures of emergency workers.

2. 10 CFR Part 50, Appendix E, including IV.E, as it relates to emergency facilities and equipment, and VI as it relates to an emergency response data system (ERDS).

3. 10 CFR 50.34(f)(2)(xxv), "Contents of applications; technical information," as it relates to providing a Technical Support Center and an Operational Support Center.

Acceptance criteria adequate to meet the above requirements include:

1. RG 1.101, Revision 5, "Emergency Planning and Preparedness for Nuclear Power Reactors"

2. NUREG-0654/Federal Emergency Management Agency (FEMA)-REP-1, Revision 1, "Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants − Final Report"

3. NUREG-0696, "Functional Criteria for Emergency Response Facilities"

4. NUREG-1394, Revision 1, "Emergency Response Data System Implementation"

5. NUREG-0737, Supplement 1, "Clarification of Three Mile Island (TMI) Action Plan Requirements"

13.3.4 Technical Evaluation

The staff reviewed FSAR Tier 2, Section 13.3, against the standards of 10 CFR 50.47(b), and applicable requirements of 10 CFR Part 50, Appendix E, as well as endorsed guidance from RG 1.101. The applicant chose to specify only design features, facilities, functions, and equipment that are technically relevant to the design and are not site-specific. Thus, the applicant did not specify:

- The design details of an emergency operations facility (EOF) as part of this FSAR, leaving these details to the COL applicant.

- A site-specific emergency plan in accordance with 10 CFR 50.47 and 10 CFR Part 50, Appendix E. Emergency planning is primarily within the scope of a COL application.

- Emergency preparedness ITAAC, as this was judged to be site-specific.

The applicant has identified the following COL information item:

- COL Information Item 13.3-1: A COL applicant that references the U.S. EPR design certification will provide a site-specific emergency plan in accordance with 10 CFR 50.47 and 10 CFR Part 50, Appendix E.

The applicant provided and the staff reviewed design features and functions of the U.S. EPR design as it relates to emergency planning. The staff reviewed the description of the space

provided for a TSC and OSC as a conceptual design. Clarification of several design features were requested via the request for additional information (RAI) process.

In RAI 24, Question 13.03-3, the staff requested that the applicant provide additional information regarding TSC size and staffing levels.

FSAR Tier 2, Section 13.3 states, "Space suitable for a technical support center, which demonstrates compliance with the design requirements for staffing levels consistent with current operating practices, and Revision 1 of NUREG-0654/FEMA REP-1, Revision 1 (Reference 2), is provided within the integrated operations area adjacent to the main control room." Refer to FSAR Tier 2, Figures 6.4-1, and 6.4-2, "Control Room Envelope Plan View 2." A detailed description of CRE habitability, including radiological protective provisions, is provided in FSAR Tier 2, Section 6.4, "Habitability Systems."

The staff requested that the applicant identify the number of work stations by function and expected occupancy levels of the TSC. The staff requested that the applicant explain whether the TSC is sized to accommodate a minimum of 25 persons, including 20 persons designated by the licensee and 5 NRC personnel. NUREG-0654 states on page 52, "Each licensee shall establish a Technical Support Center and an onsite operations support center (assembly area) in accordance with NUREG-0696…." The staff requested that the applicant determine whether the TSC meets all of the other acceptance criteria of NUREG-0696, Section 2.4. These criteria are:

- Working space, without crowding, for the personnel assigned to the TSC at the maximum level of occupancy (minimum size of working space provided shall be approximately 7 m^2/person (75 ft^2/person).
- Space for the TSC data system equipment needed to acquire, process, and display data used in the TSC.
- Sufficient space to perform repair, maintenance, and service of equipment, displays, and instrumentation.
- Space for data transmission equipment needed to transmit data originating in the TSC to other locations.
- Space for personnel access to functional displays of TSC data.
- Space for unhindered access to communications equipment by all TSC personnel who need communications capabilities to perform their functions.
- Space for storage of and/or access to plant records and historical data.
- A separate room adequate for at least three persons to be used for private NRC consultations.

In a July 25, 2008, response to RAI 24, Question 13.03-3, the applicant stated that, at a minimum, there is one process information and control system (PICS) operator workstation in the TSC. Additional workstations, such as a set of plant overview panel (POP) screens driven by another PICS workstation, may be provided at the request of the customer.

An area within the integrated operations area of at least 174.2 m^2 (1,875 ft^2) is allocated as the TSC. Thus, the TSC is large enough to provide space for 25 personnel (20 persons designated by the licensee and 5 NRC personnel) at 7 m^2 (75 ft^2) per person. Additionally, the size of the TSC 174.2 m^2 (1,875 ft^2) makes the center large enough to meet the acceptance criteria of NUREG-0696, Section 2.4. The staff finds the response provided above adequately addresses RAI 24, Question 13.03-3 and, therefore, the issue is resolved.

Generic Issues

SRP Section 13.3, "Emergency Planning," states that the majority of emergency planning requirements associated with new reactor applications are programmatic in nature and supplement physical facilities and equipment. Compliance with 10 CFR 52.47(a)(21), "Contents of applications; technical information," emergency planning features addressed in a standard design application must be technically relevant to the design (i.e., facilities and equipment) and usable for a multiple number of units or at a multiple number of sites. In general, programmatic aspects of emergency planning and preparedness are the responsibility of the COL applicant that references the certified standard design.

As stated in 10 CFR 52.47(a)(21), the standard design application must include proposed technical resolutions of those Unresolved Safety Issues and medium- and high-priority generic safety issues, which are identified in the version of NUREG-0933, "A Prioritization of Generic Safety Issues," current on the date up to 6 months before the docket date of the application (August 2004 is current version), and which are technically relevant to the design.

Generic Letter (GL) 82-33, "Supplement 1 to NUREG-0737 - Emergency Response Capabilities," provides clarification regarding emergency response capability; including applicability of RG 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident," Revision 4, June 2006, to emergency response facilities.

RG 1.97 describes acceptable methods for conforming with agency regulations relating to criteria for accident monitoring instrumentation. Additional detailed design and functional criteria relating to the TSC, OSC, and EOF are provided in NUREG-0696.

In RAI 24, Question 13.03-7, the staff requested that the applicant provide additional information regarding Generic Issues. The staff requested clarification on whether the U.S. EPR design contains instrumentation for following the course of an accident that meets all of the above referenced guidance for the TSC and OSC. The staff requested a justification from the applicant if it did not meet this guidance. Since no mention was made of the EOF in the FSAR, this was considered outside the scope of the U.S. EPR design and, thus, left to the COL applicant to specify.

In a July 25, 2008, response to RAI 24, Question 13.03-7, the applicant stated that, through the PICS workstation, the technical support center has display capabilities for the post-accident monitoring variables specified in RG 1.97. There are no regulatory requirements to provide live data and status information in the OSC. The EOF is outside the scope of the U.S. EPR design certification. Details of the EOF will be provided in the site-specific emergency plan provided by the COL applicant per COL Information Item 13.3-1: "A COL applicant that references the U.S. EPR design certification will provide a site-specific emergency plan in accordance with 10 CFR 50.47 and 10 CFR Part 50, Appendix E." The staff finds the response provided above adequately addressed RAI 24, Question 13.03-7 and, therefore, the issue is resolved.

13.3.5 Combined License Information Items

Table 13.3-1 provides a list of emergency planning related COL information item numbers and descriptions from FSAR Tier 2, Table 1.8-2:

Table 13.3-1 U.S. EPR Combined License Information Items

Item No.	Description	FSAR Tier 2 Section
13.3-1	A COL applicant that references the U.S. EPR design certification will provide a site-specific emergency plan in accordance with 10 CFR 50.47 and 10 CFR 50 Appendix E.	13.3

The staff finds the above listing to be complete. Also, the list adequately describes actions necessary for the COL applicant or holder. No additional COL information items need to be included in FSAR Tier 2, Table 1.8-2 for emergency preparedness.

13.3.6 Conclusions

Based upon the above responses to the RAIs specified in the "Technical Evaluation" Section 13.3.4 above, the staff concludes that the information provided in the FSAR pertaining to emergency preparedness conforms to the guidance provided in RG 1.101. The staff determined that the FSAR is in compliance with the applicable standards set out in 10 CFR 50.47(b) and 10 CFR Part 50, Appendix E, Section IV.E, insofar as it describes the essential elements of advanced planning and the provisions made to cope with emergency situations, as set forth above.

13.4 Operational Program Implementation

13.4.1 Introduction

The applicant has identified the design areas and sections of the FSAR that support operational programs. A COL applicant that references the U.S. EPR design certification will provide the site-specific information for these operational programs and a schedule for implementation.

13.4.2 Summary of Application

FSAR Tier 1: There are no FSAR Tier 1 entries for this area of review.

FSAR Tier 2: The applicant has not provided an FSAR Tier 2 program description in Section 13.4, "Operational Program Implementation," of the FSAR.

Operational programs required to be implemented by regulation are given in this section of the FSAR. The applicant lists the following 11 operational programs that are described in other sections of the FSAR and for which a COL applicant will verify and provide the implementation schedule:

- Inservice inspection program (refer to FSAR Tier 2, Sections 5.2.4, “Inservice Inspection and Testing of the RCPB,” and 6.6, “Inservice Inspection of Class 2 and 3 Components”)

- Inservice testing program (refer to FSAR Tier 2, Sections 3.9.6, “Functional Design, Qualification, and Inservice Testing Programs for Pumps, Valves, and Dynamic Restraints,” and 5.2.4)

- Environmental qualification program (refer to FSAR Tier 2, Section 3.11, “Environmental Qualification of Mechanical and Electrical Equipment”)

- Preservice inspection program (refer to FSAR Tier 2, Sections 5.2.4 and 6.6)

- Reactor vessel material surveillance program (refer to FSAR Tier 2, Section 5.3.1, “Reactor Vessel Materials”)

- Preservice testing program (refer to FSAR Tier 2, Sections 3.9.6 and 5.2.4)

- Containment leakage rate testing program (refer to FSAR Tier 2, Section 6.2.6, “Containment Leakage Testing”)

- Fire protection program (refer to FSAR Tier 2, Section 9.5.1, “Fire Protection System”)

- Process and effluent monitoring and sampling program (refer to FSAR Tier 2, Section 11.5, “Process and Effluent Monitoring and Sampling Systems”)

- Motor-operated valve testing (refer to FSAR Tier 2, Section 3.9.6)

- Initial test program (refer to FSAR Tier 2, Section 14.2, “Initial Plant Test Program”)

In addition, the FSAR lists eight operational programs that the COL applicant will both describe and provide an implementation schedule. These include:

- Training program for non-licensed plant staff (refer to FSAR Tier 2, Section 13.2)

- Training program for reactor operators (refer to FSAR Tier 2, Section 13.2)

- Reactor operator requalification program (refer to FSAR Tier 2, Section 13.2)

- Emergency planning (refer to FSAR Tier 2, Section 13.3)

- Security program (refer to FSAR Tier 2, Section 13.6, “Security”)

- Operational quality assurance program (refer to FSAR Tier 2, Section 17.5, “Quality Assurance Program Description”)

- Radiation protection program (refer to FSAR Tier 2, Section 12.5, “Operational Radiation Protection Program”)

- Maintenance rule (refer to FSAR Tier 2, Section 17.6, “Description of Applicant's Program for Implementation of 10 CFR 50.65, the Maintenance Rule”)

- Cyber security plan (refer to FSAR Tier 2, Section 13.6, “Security”) (Confirmatory Item 14.03.05-3)

ITAAC: There are no ITAAC items for this area of review.

13.4.3 Regulatory Basis

The relevant requirements of NRC regulations for this area of review, and the associated acceptance criteria, are given in NUREG-0800, Section 13.4 and are summarized below. Review interfaces with other SRP sections also can be found in NUREG-0800, Section 13.4.

- 10 CFR 52.79, “Contents of Applications; Technical Information in Final Safety Analysis Report,” as it relates to fully describing certain operational programs and their implementation.

Acceptance criteria adequate to meet the above requirements include:

- SECY-05-0197

13.4.4 Technical Evaluation

In the Staff Requirements Memoranda (SRM) for SECY-05-0197, the Commission provided the following directions regarding operational programs:

- Identify the list of operational programs required to be included in a COL application.

- Include license conditions for operational programs in the COL, where implementation requirements are not specified in the regulations.

- Use proposed generic emergency planning/emergency preparedness ITAAC as a model for EP ITAAC to be included in COL applications.

In the SRM regarding SECY-05-0197, the Commission also endorsed the staff’s proposal that an operational program does not require ITAAC in the COL application, provided that the application “fully describes” the program and its implementation. Thus, to avoid the need to propose ITAAC for a given operational program, the COL applicant must fully describe both of the following:

- Operational program

- Implementation of the operational program

In the SRM for SECY-04-0032, “Programmatic Information Needed for Approval of a Combined License Without Inspections, Tests, Analyses and Acceptance Criteria,” May 14, 2004, the Commission defined “fully described” as follows:

> In this context, "fully described" should be understood to mean that the program is clearly and sufficiently described in terms of scope and level of detail to allow a reasonable assurance finding of acceptability. Required programs should always be described at a functional level and at an increased level of detail where implementation choices could materially and negatively affect the program effectiveness and acceptability.

This definition of "fully described" is reiterated in the Statements of Consideration associated with the revised 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," August 28, 2007. Toward that end, the COL FSAR Section 13.4 should provide a table that lists each operational program, the sections of the COL FSAR that fully describe the operational program, and the associated implementation milestones.

The staff's review of the 11 operational program descriptions provided in the applicable FSAR Tier 2 sections have been performed as part of the review of those FSAR sections. The design certification applicant intended to "fully describe" some of these programs. The staff's evaluation of these programs and the staff's decision on whether these programs were fully described, as discussed above, will be documented in those FSAR sections. The COL applicant will verify and provide the implementation schedule for these programs. This is acceptable to the staff.

In RAI 78, Question 14.03.05-3, the staff requested that the applicant demonstrate how ITAAC addresses the digital safety system security guidance provided in Revision 2 of RG 1.152, "Criteria for Use of Computers In Safety Systems of Nuclear Power Plants." ITAAC should verify that the application conforms to Regulatory Positions 2.1-2.9 in RG 1.152, and address cyber security. In an October 3, 2008, response to RAI 78, Question 14.03.05-3, the applicant stated, in part, that it believes that the waterfall lifecycle phases described in RG 1.152, Revision 2, Regulatory Positions 2.1 through 2.9 for the protection of digital safety systems are intended to be controlled through the cyber security program required by 10 CFR 73.54(d). This consideration is consistent with the provisions in RG 5.71, Revision 0, January 2009, Section 3.4.1.1.1, "Life Cycle Phases Activities." RG 5.71 states: "The licensees bears sole responsibility for ensuring that the potential for adverse effects on safety, security, and emergency preparedness is assessed and managed to provide a high assurance that critical functions are adequately protected from cyber attacks." Thus, FSAR Tier 1, ITAAC does not explicitly address the cyber security design. To incorporate the requirements of 10 CFR 73.54 (74 *Federal* Register (FR) 13970, March 27, 2009), FSAR Tire 2, Table 1.8-2 and FSAR Tire 2, Section 13.6 will be revised to include a new COL Information Item (13.6-4) incorporating a new operational program: "A COL applicant that references the U.S. EPR design certification will provide a cyber security plan consistent with 10 CFR 73.54." FSAR Tier 2, Section 13.4 will also be revised to include the new operational program. The staff finds this response to be acceptable with respect to creating a new COL information Item to provide a cyber security plan consistent with 10 CFR 73.54, and to add this new program to the list of operational programs in FSAR Tier 2, Section 3.4. **RAI 78, Question 14.03.05-3 is being tracked as a confirmatory item**.

13.4.5 Combined License Information Items

Table 13.4-1 provides a list of operational program related COL information item numbers and descriptions from FSAR Tier 2, Table 1.8-2:

Table 13.4-1 U.S. EPR Combined License Information Items

Item No.	Description	FSAR Tier 2 Section
13.4-1	A COL applicant that references the U.S. EPR design certification will provide site-specific information for operational programs and schedule for implementation.	13.4

The staff finds the above list of COL information items to be complete, and adequately describes the actions necessary for the COL applicant or holder. No additional COL information items need to be included in FSAR Tier 2, Table 1.8-2 for operational program implementation consideration.

13.4.6 Conclusions

The staff finds the operational programs listed in FSAR Tier 2, Section 13.4 to be acceptable, in accordance with 10 CFR 52.79.

13.5 Plant Procedures

13.5.1 Introduction

FSAR Tier 2, Section 13.5, "Plant Procedures," addresses the procedures, including administrative, that will be used by the plant staff to ensure that routine operating, off-normal, and emergency activities are conducted in a safe manner. Descriptions of the content and development process for these procedures are included in the FSAR. Detailed written procedures are not included, as development of detailed procedures and associated training materials are beyond the scope of the application for design certification and are the responsibility of the COL applicant. The staff will inspect the procedures as part of the Construction Inspection Program.

13.5.2 Summary of Application

FSAR Tier 1: There are no FSAR Tier 1 entries for this area of review.

FSAR Tier 2: The applicant has provided an FSAR Tier 2 program description in Section 13.5, summarized here, in part, as follows:

A COL applicant that references the U.S. EPR design certification will provide site-specific information for administrative, operating, emergency, maintenance, and other operating procedures. The FSAR addresses emergency operating procedures content, the emergency operating procedures development process, procedures generation packages, and procedures development acceptance criteria. Additional information for a COL applicant to prepare administrative, operating, emergency, maintenance, and other operating procedures is provided in FSAR Tier 2, Chapter 18.

ITAAC: There are no ITAAC items for this area of review.

Technical Specifications: The Technical Specifications associated with FSAR Tier 2, Section 13.5, are given in FSAR Tier 2, Chapter 16, Section 5.4, "Procedures."

Plant Interfaces: This section of the FSAR contains information related to the following plant interfaces that will be addressed in the COL designs: See Table 1.8-1, "Summary of U.S. EPR Plant Interfaces with Remainder of Plant," Item 13-1, "Site-specific information for administrative, operating, emergency, maintenance, and other operating procedures."

13.5.3 Regulatory Basis

The relevant requirements of NRC regulations for this area of review and the associated acceptance criteria are given in NUREG-0800, Sections 13.5.1.1 and 13.5.2.1 and are summarized below:

1. 10 CFR 50.34(f)(3)(i), "Contents of Applications; Technical information," as it relates to the development, verification and validation, implementation, and maintenance of revision of plant procedures.

2. 10 CFR 50.40(a) and (b), "Common Standards," insofar as it requires that the applicant adhere to certain established standards and be technically qualified to engage in proposed activities. This section also relates to how the administrative procedures program contributes to the determination whether an applicant is technically qualified by putting in place necessary controls, policies, and programs for appropriate and controlled activities as required by 10 CFR Part 50, Appendix A, Criterion 1, and Appendix B, Criterion XI.

3. 10 CFR Part 50, Appendix B, Criteria V and VI, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," as it requires that activities affecting quality be prescribed by documented instructions, procedures, and drawing and that measures be established to control issues of and changes to these documents.

Review interfaces with other SRP sections are listed in NUREG-0800, Sections 13.5.1.1 and 13.5.2.1.

Acceptance criteria adequate to meet the above requirements include:

1. RG 1.33, "Quality Assurance Program Requirements (Operation)"

2. NUREG-0694, "TMI-Related Requirements for New Operating Licenses"

3. NUREG-0737, "Clarification of TMI Action Plan Requirements"

4. NUREG-0578, "TMI-2 Lessons Learned Task Force Status Report and Short-term Recommendations"

5. NUREG-0711, "Human Factors Engineering Program Review Model"

6. NUREG-1358, Supplement 1, “Lessons Learned from the Special inspection Program for Emergency operating Procedures,” 1992

7. NUREG-0737, Supplement I, “Requirements for Emergency Response Capability"

13.5.4 Technical Evaluation

In FSAR Tier 2, Section 13.5, the applicant stated that a COL applicant referencing the U.S. EPR certified design will provide site-specific information for administrative, operating, emergency, maintenance and other operating procedures. This is COL Information Item 13.5-1. The staff also discusses its evaluation of plant procedures in Section 18.9 of this report. There are no areas where additional information needs to be provided in the design certification application.

13.5.5 Combined License Information Items

Table 13.5-1 provides a list of plant procedures related COL information item numbers and descriptions from FSAR Tier 2, Table 1.8-2:

Table 13.5-1 U.S. EPR Combined License Information Items

Item No.	Description	FSAR Tier 2 Section
13.5-1	A COL applicant that references the U.S. EPR design certification will provide site-specific information for administrative, operating, emergency, maintenance, and other operating procedures.	13.5

The staff finds the above list of COL information items to be complete, and adequately describes the actions necessary for the COL applicant or holder. No additional COL information items need to be included in FSAR Tier 2, Table 1.8-2 for plant procedures consideration.

13.5.6 Conclusions

In FSAR Tier 2, Section 13.5, the applicant stated that a COL applicant referencing the U.S. EPR certified design will provide site-specific information for administrative, operating, maintenance, and emergency operating procedures. The procedures program is not within the scope of the U.S. EPR design certification and will be provided on a site-specific basis by each COL applicant referencing the U.S. EPR design. The staff will review the procedures program in the context of each COL application, and this is acceptable. The staff will inspect the procedures themselves, as written, as part of the Construction Inspection Program.

13.6 Security

13.6.1 Introduction

The FSAR and referenced technical reports describe the physical protection systems that are within the scope of the U.S. EPR standard design for a nuclear power plant, including plant

layout and configurations, to establish a design standard that will provide physical protection functions for detection, assessment, communications, delay, and responses to protect against acts of radiological sabotage and theft of special nuclear material.

Specifically, the FSAR provides design descriptions addressing the vital island and vital structures of the U.S. EPR, identification of vital equipment and area boundaries, and design descriptions of physical protection systems that are within the scope of the design certification. FSAR Tier 1 and FSAR Tier 2 docketed information, and referenced AREVA NP Technical Report (TR) ANP-10295, "U.S. EPR Security Features," provide the conceptual, functional, detailed design and performance requirements, along with supporting technical bases, that a combined license applicant will incorporate by reference in its application. Together with additional site-specific physical protection systems (engineered and administrative controls) to establish a protective strategy, and security organization, and programs, the design described in the U.S. EPR FSAR will meet requirements of 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage." TR ANP-10295 contains safeguards information (SGI) and is protected in accordance with requirements of 10 CFR 73.21, "Requirements for the Protection of Safeguards Information."

The physical protection structures, systems, and components that are not within the scope of the certified design are required by 10 CFR Part 73, and will be addressed by a COL applicant that references the U.S. EPR certified design by means of COL Information Items Nos. 13.6-1 through 13.6-4. The FSAR includes COL Information Item No. 13.6-2 which states that a COL applicant that references the U.S. EPR design certification will provide a security plan to the NRC to fulfill the requirements of 10 CFR 52.79. The security plan will consist of physical protection, contingency, and training and qualification plans.

13.6.2 Summary of Application

FSAR Tier 1: FSAR Tier 1, Chapter 3, "Non-System Based Design Descriptions and ITAAC," Section 3.1, "Physical Protection System," describes physical protection design features, interface requirements, and inspections, tests, analyses, and acceptance criteria for physical protection systems and hardware for the U.S. EPR standard design. The design descriptions include the figures in FSAR Tier 1, where the figures are intended to depict the functional arrangement of the significant structures, systems, and components of the standard design.

FSAR Tier 2: The applicant provided a description of the physical protection system in FSAR Tier 2, Section 13.6, "Security," summarized here, in part, as follows:

FSAR Tier 2, Section 1.2, "General Plant Description," and Section 1.2.3, "Plant Description," of the FSAR provide descriptions of the scope of the U.S. EPR standard design. FSAR Tier 2 of the application includes design descriptions for physical protection systems within the scope of the design certification and those portions of the plant that are outside the scope of the U.S. EPR standard design, and as such are designated as out-of-scope in various places in the FSAR Tier 2 information. The portions of the U.S. EPR standard design for which design information is included in the FSAR Tier 2 information are identified and specified in FSAR Tier 2, Section 1.8, "Interfaces with Standard Designs and Early Site Permits."

FSAR Tier 2, Section 13.6 references TR ANP-10295, which describes the design and performance of physical protection systems that are within the scope of design certification and the conceptual design for physical protection systems that would be further developed by a

COL applicant. For example, the applicant also described the design and configuration of physical protection systems, such as perimeter intrusion detection systems, surveillance and assessment systems, vehicle barrier systems (VBSs), protected area security lighting, perimeter defensive fighting positions, personnel and vehicle access control portal, and barriers for protection of protected area (PA) penetrations, that are beyond the physical boundary of the Nuclear Island and structures. The conceptual designs for these physical protection systems or features, which are independent of the physical protection systems for the vital island and structures, are not included in the design certification of the U.S. EPR, and the staff has not reviewed them. The descriptions of site-specific physical protection system design is to be prepared and submitted by a COL applicant under COL Information Item Nos. 13.6-1 through 13.6-6. A COL applicant referencing the U.S. EPR design will describe the plans for engineered systems, administrative controls, management control and processes, and programs for the protection of the nuclear power plant in accordance with 10 CFR Part 73, "Physical Protection of Plants and Materials. FSAR Tier 2, Section 1.8.1, "COL Information Items," FSAR Tier 2, Tables 1.8-1, and 1.8-2, "U.S. EPR Combined License Information Items," include discussions of ITAAC specific to the physical protection system. In the same chapter, FSAR Tier 2, Section 1.9.1, "Conformance with Regulatory Guides," (Table 1.9-2, "U.S. EPR Conformance with Regulatory Guides") identifies Division 5 regulatory guides applicable to physical protection that were considered or incorporated by reference in the U.S. EPR standard design.

FSAR Tier 2, Section 13.6 describes physical protection system features incorporated in the U.S. EPR standard design. The design of physical protection systems beyond the scope of the standard design certification and elements of a security program, such as organization structure, training, operational program implementations, plant procedures, credited operator actions for target sets, physical protection system assessments and analyses, protective strategy against the design-basis threat (DBT), design of site-specific features for physical protection system, and access authorization and fitness for duty program, are to be described by the COL applicant, along with operational programs implementing schedule and milestones. TR ANP-10295 and TR ANP-10296, "U.S. EPR Design Features that Enhanced Security," are FSAR Tier 2 documents referenced in Section 13.6 to provide details and technical bases for the design and assumptions for physical protection systems and features incorporated into the U.S. EPR standard design. TR ANP-10295 contains information that is safeguards and security-related, and is protected in accordance with 10 CFR 73.21 and 10 CFR 2.390, "Public Inspections, Exemptions, Requests for Withholding," respectively. TR ANP-10296 provides information and descriptions of how the U.S. EPR standard design incorporates and considers standards and objectives for physical protection of the Nuclear Island, vital structures, and certain other structures, systems, and components.

The physical protection systems and hardware that will be verified to satisfy the acceptance criteria using inspections, tests, or analyses are discussed in FSAR Tier 2, Chapter 14, "Verification Programs," Section 14.3, "Inspection, Test, Analysis, and Acceptance Criteria," and FSAR Tier 2, Table 14.3-8, "ITAAC Screening Summary." In addition, FSAR Tier 2, Section 14.2.10.1, "Initial Fuel Loading," discusses minimum initial conditions for core load that include establishing the physical protection system prior to fuel loading. FSAR Tier 2, Section 14.2.12.10.7, "Physical Protection System Lighting (Test No. 114)," and FSAR Tier 2, Section 14.2.12.11.7, "Communication System (Test No. 130)," and associated Table 14.2-1, "List of Initial Tests for U.S. EPR," address physical protection systems and components of a plant's lighting and intra-plant communications. The descriptions of inspection objectives, test

methods, and acceptance criteria (i.e., test abstracts) supporting physical protection systems ITAAC described in FSAR Tier 1 are described in TR ANP-10295.

ITAAC: FSAR Tier 1, Table 3.1-1, "Security ITAAC," describes the ITAAC for physical protection system hardware that are within the scope of the U.S. EPR standard design.

Interface Requirements: This section of the FSAR contains information related to interface requirements that will be addressed by the COL applicant. FSAR Tier 2, Table 1.8-1 provides a summary of U.S. EPR plant interface with the remainder of the plant. FSAR Tier 2, Table 1.8-1, Item 13-3, identifies the site-specific security assessment and Physical Security Plan as an interface between the U.S. EPR standard design and the remainder of the plant.

13.6.3 Regulatory Basis

The relevant requirements of NRC regulations for this area of review, and the associated acceptance criteria, are specified in NUREG-0800, Sections 13.6, "Physical Security," and 13.6.2, "Physical Security − Design Certification," and are summarized below:

1. 10 CFR Part 73, which specifies performance-based and prescriptive regulatory requirements that, when adequately met and implemented provide protection of nuclear power reactors against acts of radiological sabotage, prevent the theft or diversion of special nuclear material, and protect safeguards information against unauthorized release.

2. 10 CFR 73.55(b), "General Performance Objective and Requirements," which requires an applicant to establish and maintain an onsite physical protection program 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.

3. 10 CFR 73.55(b)(2), establishes the performance-based regulatory requirement to protect a nuclear power plant against the design-basis threat of radiological sabotage as described in 10 CFR 73.1(a)(1), "Radiological Sabotage."

Acceptance criteria adequate to meet the above requirements include those set forth in:

1. RG 5.7, "Entry/Exit Control for Protected Areas, Vital Areas, and Material Access Areas," Revision 1, May 1980

2. RG 5.12, "General Use of Locks in the Protection and Control of Facilities and Special Nuclear Materials," November 1973

3. RG 5.44, "Perimeter Intrusion Alarm Systems," Revision 3, October 1997

4. RG 5.65, "Vital Area Access Controls, Protection of Physical Protection System Equipment and Key and Lock Controls," September 1986

5. 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," June 2006

6. RG 5.74, “Managing the Safety/Security Interface,” March 2009

7. RG 5.75, “Training and Qualification of Security Personnel at Nuclear Power Reactor Facilities,” June 2009

8. RG 5.76, “Physical Protection Programs at Nuclear Power Reactors,” July 2009

9. RG 5.77, “Insider Mitigation Program (IMP),” March 2009

10. RG 1.206, “Combined License Applications for Nuclear Power Plants (LWR Edition),” June 2007

13.6.4 Technical Evaluation

The staff reviewed the design descriptions of physical protection systems in the application and the elements considered with respect to physical protection in the design of the buildings, structures, systems, and components that are within the scope of design certification, as described in the FSAR, to determine whether they satisfy the requirements of 10 CFR Part 73. For the physical protection system features that have been incorporated as part of the design certification, the staff’s review consisted of determining whether the applicant has provided adequate and reasonable descriptions of design and technical bases, and has described how the proposed design will facilitate the implementation of a comprehensive physical protection system (i.e., engineered and administrative controls) and physical protection program. The staff reviewed the program to determine whether it would provide high assurance of adequate protection against radiological sabotage in accordance with adversarial characteristics of the design basis threat stated in 10 CFR 73.1(a)(1) and meet requirements for physical protection, as specified in 10 CFR 73.55(a), “Introduction,” through 10 CFR 73.55(r), “Alternative Measures.”

The staff’s review also included the review of identified COL information items for the U.S. EPR design to determine specific actions or design of physical protection systems and programs that will be addressed by all COL applicants who reference the U.S. EPR as a standard design.

The staff’s review and scope was limited to the adequacy of the design basis and assumptions for the physical protection systems and components that are relied on to implement security response functions (i.e., detection, assessment, communications, delays, and neutralization). The demonstration of a high assurance of adequate protection against the DBT and compliance with programmatic requirements (including administrative controls such as people and procedures) of 10 CFR Part 73 are to be addressed by a COL applicant who is seeking a combined license for a nuclear power facility. A regulatory determination on the adequacy of programmatic or administrative controls planned for meeting 10 CFR Part 73 will not be made during a design certification review and will be reserved for review of a COL application.

The staff’s review also includes AREVA responses submitted to the NRC as stated in RAIs 42, 92, 246, 247, and 253 (and resulting revisions to the FSAR or referenced technical reports) on the design basis and technical assumptions related to physical protection systems incorporated as standard design for certification:

- AREVA NP, TR ANP-10295 (AREVA NP, TR ANP-10296 Safeguards Information (SGI)), “U.S. EPR Security Features,” Revision 0, submitted on December 5, 2008, supplemented by Revision 1, October 28, 2009

- AREVA NP to the NRC, "Response to U.S. EPR Design Certification Application RAI No. 42, Supplement 1," December 9, 2008

- AREVA NP to the NRC, "Response to U.S. EPR Design Certification Application RAI No. 92, Supplement 1," December 5, 2008

- AREVA NP to the NRC, "Response to U.S. EPR Design Certification Application RAI No. 246, Supplement 1," dated October 28, 2009

- AREVA NP to the NRC, "Response to U.S. EPR Design Certification Application RAI No. 247, Supplement 1," October 28, 2009

- AREVA NP to the NRC, "Response to U.S. EPR Design Certification Application RAI No. 253, Supplement 1," October 28, 2009

- AREVA NP to the NRC, "Response to U.S. EPR Design Certification Application RAI No. 78, Supplement 2," June 12, 2009

13.6.4.1 *Design Considerations for Physical Protection*

In TR ANP-10295 the applicant states that it considered and incorporated into the U.S. EPR standard design, physical protection systems or features to enhance implementation of physical protection of the reactor power plant against the DBT and the implementation of a physical protection programs. Specifically, the FSAR describes what and how engineered physical protection systems or features, including configurations and layout of the U.S. EPR standard plant footprint and access points, have been incorporated to provide, facilitate, or enhance capabilities to detect, assess, communicate, delay, and interdict malevolent acts that are bounded by the adversarial characteristics associated with the DBT. The information in FSAR Tier 2 describes the standard physical protection features incorporated into the U.S. EPR standard design.

The applicant's TR ANP-10295 provides detailed descriptions of the design and performance of systems configurations for design features identified in FSAR Tier 1, Section 3.1.1, "Design Features." The design descriptions include design bases assumptions, and requirements for physical protection systems. The reliability and availability of physical protection systems are discussed in the design bases and technical assumptions. The applicant's analyses and evaluations establish the design bases for physical protection features incorporated in the U.S. EPR standard design.

The applicant indicates that a majority of the general design concepts of NRC NUREG/CR-1345, "Nuclear Power Concept for Sabotage Protection," January 1981, to protect critical systems/locations, plant layout, system design, and generic and PWR design changes, have been incorporated into the U.S. EPR design and are documented in the applicant's TR ANP-10296.

In TR ANP-10296, the applicant describes the following design features, which are intended to enhance physical protection of the U.S. EPR standard design:

- The U.S. EPR standard design includes a robust or hardened Shield Building consisting of layered structural materials, which have been incorporated in the

design of the Containment, Safeguard, and Fuel Buildings to provide protection against external hazards, including impact from a large commercial aircraft. The walls are designed to prevent penetration of the structures and protect personnel and equipment.

- The Shield Building encases the structure where the control and safety-related systems and equipment reside. Independent divisions of safety-related systems are located in separate buildings, and divisions of safety-related systems are spatially separated to ensure that a single event cannot affect redundant divisions.

- The U.S. EPR incorporates a four safety-division design. The applicant assumes in engineering analyses that one division may be in a maintenance outage, one division fails to actuate because of the event, and two divisions are available and operational to perform their intended safety function. In the cases where a component fails and the event potentially impacts two divisions, that analysis would result in assuming one division out for maintenance, two divisions damaged by the event, and one division to perform its intended safety function. The applicant postulates at least one fully functional division remains available to provide defense-in-depth for safety by design.

- Four safety-divisions cables, piping, and control circuits, are routed from vital structures into the Nuclear Island through penetrations that are spatially and physically separated. The emergency core cooling system (ECCS) division electrical and control cables are separately routed through cable pathways to the main control room and remote shutdown station.

- The configuration of safety-related systems for core cooling are spatially separated such that one event cannot disable more than two divisions. Each division of safety-related systems provides independent post-trip decay heat removal to stabilize the reactor in hot shutdown conditions. Each of the four divisions, hardened by the Shield Building and spatially separated, has hours of decay heat removal capability. Therefore, the total system can provide capabilities (as described in TR ANP-10296) for hours of operations before makeup is necessary.

- Dedicated emergency diesel generators and station blackout diesel generators provide power. The SBODGs are independent of external cooling water, use an alternative cooling method, and have a dedicated fuel oil tank. The SBODG will provide supplemental power should emergency diesel generators (EDGs) fail to start and to support systems not powered by the emergency diesels. The SBODG will automatically power a minimum of two emergency buses for an alternate feed, as described in, Chapter 8, “Electric Power,” of this report, and are designed to align to the remaining emergency buses. The EDGs are provided with dedicated fuel oil tanks that are spatially separated and independent within protective enclosures. There are a number (as described in TR ANP-10296) of diesel generators, each capable of providing 100 percent power for safe shutdown.

- Several dedicated independent safety-related system divisions (as described in TR ANP-10296) are designed with heat sinks to transfer decay heat and maintain spent fuel pool cooling. The safety-related systems are within hardened structures and collectively contain a large quantity of water (as described in TR ANP-10296) for decay heat removal for the duration of many days without makeup water from external intake structures. The applicant stated that the design provides for sufficient water within the safety-related systems for 15 to 30 days, depending on time since the last refueling, under hot standby conditions with credited electrical loads. Additional action by the Emergency Response Organization during the first 15 days provides for replenishing the water in the ESW basins to support extended operations, if needed.

- The standard U.S. EPR design includes automatic initiation of safety-related systems to provide core cooling, and structures, systems, and components, including protection systems, designed to minimize operator actions. Several divisions of safety-related systems are credited for fast cool down (FCD), and credited for partial cool down (PCD) functions and initial decay heat removal to reach and maintain hot standby. Operator and emergency response organization actions are credited for long-term operations.

- The U.S. EPR standard design is equipped with a dedicated spreading compartment and system to retain and cool molten core debris, including the entire core inventory, reactor internals, and residual portions of the lower vessel head, using the in-containment water storage tank water to stabilize molten corium prior to a challenge of containment integrity.

- Independent pressurizer spray divisions for coolant loops, with a separate emergency power and emergency depressurization system to reduce pressure to allow medium head safety injection, are provided by design.

- The spent fuel pool cooling system (FPCS) divisions are isolated to provide spatial separation and redundant capabilities for spent fuel cooling spray system.

- The U.S. EPR standard design also improved on past designs to address pipe ruptures and backflow protection by incorporating at least two check valves or two isolation valves on each line with direct RCS connection.

The applicant concludes that the multiple divisions, reinforced structures, robust external doors, and spatial separation of divisions are design elements that provide significant protection against external hazards and hostile actions.

In RAI 42, Question 14.03.12-3, the staff requested that the applicant provide a discussion and appropriate detailed information regarding approaches or concepts (e.g., protection-in-depth) for physical protection considered and applied in the standard EPR design. In a December 9, 2008, response to RAI 42, Question 14.03.12-3, the applicant indicated that TR ANP-10295 provides discussions and detailed information on approaches or concepts (e.g., defense-in-depth) for physical protection considered and applied in the U.S. EPR design. TR ANP-10296 provides a discussion of how the U.S. EPR addresses the recommendations contained in NUREG/CR-1345.

TR ANP-10295 provides detailed information to supplement the information in FSAR Tier 2. It also describes the detailed information that the COL applicant will submit to address COL Information Item Nos. 13.6-1 and 13.6-3. Design-related information, results of evaluations or analyses, and design and performance assumptions for physical protection systems and features included in the TR ANP-10295 are:

- Identification of vital equipment and vital areas for the U.S. EPR standard design
- Security power system (interior and exterior lighting, primary and secondary power supply)
- Bullet resistant enclosures
- Vehicle barrier system analyses (vital island and structures blast calculations, air-blast leakage, external equipment doors, and blast standoff distances)
- Defensive positions (internal and access to vital structures)
- Delay features (internal to vital structures)
- Surveillance and monitoring
- Alarm stations
- Insider mitigation (design features and systems relied on for program implementation)

TR ANP-10295 also describes physical protection system test abstracts that establish the framework for ITAAC verification and cyber security consideration for physical protection systems.

The staff concludes as follows:

- The U.S. EPR standard design includes the following features to enhance physical protection: Hardening of building structure (e.g., shielding building, reinforced concrete constructions, etc.); independence and redundancy of dedicated safety equipment; configuration and spatial separation of safety and security structures, systems, and components (e.g., four independent safety divisions, central alarm station (CAS), and secondary alarm station (SAS)); redundancy of primary and secondary power for safety and security systems, design improvements for pipe ruptures and backflow protection, automated protection system,; and core cooling system.
- The staff concludes that the independence, redundancy, and spatial separation of vital structures and safety-related structures, systems, and components for the U.S. EPR standard design enhance or facilitate the design of a physical protection system by: 1) Increasing the number tasks, sequences of tasks, and task times for DBT adversaries to cause failures or loss of safety-functions that could lead to radiological sabotage; 2) providing hardening and configurations of the vital island and structures that can be credited for the physical protection

functions of delay, bullet resistance, access control, and explosive blast protection; 3) providing spatial separation that minimizes or prevents a single event or act from causing failure or loss of all safety or security functions; and 4) providing a standard plant configuration that would allow a layered defense or defense-in-depth protection within the vital island and structures to interdict and neutralize DBT adversaries.

- The applicant has reasonably considered protection against radiological sabotage, by application of technical guidance available, such as NRC NUREG/CR-1345, in the standard design to harden structures, and to enhance locations or layout, and the design for protection of safety-related systems. The staff concludes that the applicant has adequately considered in the U.S. EPR standard design the applicable requirements for the design of a physical protection system as stated in 10 CFR 73.55 for the portion of the design within the scope of the certification application, in accordance with 10 CFR Part 52.

13.6.4.2 *Physical Protection System Evaluations and Analyses*

13.6.4.2.1 Vital Equipment

The processes to determine a complete and accurate set of vital equipment of the U.S. EPR standard design and the resulting list of vital equipment and designated vital areas are described in TR ANP-10295, Appendix A, "Vital Equipment List."

In TR ANP-10295, the applicant states that "it considered the probabilistic risk assessment (PRA) and risk insights from various assessments, such as fires and flooding, in the determination of vital equipment." The applicant indicates that it applied NRC NUREG-1178, "Vital Equipment/Area Guideline Study: Vital Area Committee Report," to provide the conditions under which the vital equipment were selected. The process includes identifying equipment using the assumptions of NUREG-1178 and is aided by evaluations performed to identify a safe-shutdown list. The safe-shutdown list only considered safety-related equipment to support the guidance Branch Technical Position (BTP) 5-4, "Design Requirements of the Residual Heat Removal System." Thermal-hydraulic and safety-analysis calculations were reviewed to verify equipment selected was appropriate and capable of meeting the required end state. The applicant indicates that the appropriate system description documents (SDDs), electrical load listing, electrical one-line diagrams, and piping and instrumentation diagrams (P&IDs) were used to verify the selected equipment capabilities and features. Supporting systems were identified based on interface documents and were included in the Vital Equipment List. Finally, the process includes review of general design-related documents along with SDDs which were used to identify equipment physical location.

The following is a summary of the applicant's assumptions and descriptions of the process applied to identify a list of vital equipment (and vital areas):

- "All of the components maintained on the Vital Equipment List are NOT required to complete a shutdown. Typically, one division of safety-related equipment is required, unless noted." The safety-related systems and components for reactivity control, reactor coolant makeup, coolant system pressure control, decay heat removal, and process monitoring are functions associated with reaching and maintaining a safe-shutdown condition.

- The 13 assumptions from NUREG-1178, as stated below, were considered in the process for identifying vital equipment. In summary, the applicant's assumptions include the following:

    - Assumption 1: "For protection against radiological sabotage, the primary coolant pressure boundary consists of the reactor vessel and reactor coolant piping up to and including a single, protected, normally-closed isolation valve or protected valve capable of closure in interfacing system."

    - Assumption 2: "Any transient or event that causes significant core damage will result in a 10 CFR Part 100 [10 CFR 52.47(a)(2)]release."

    - Assumption 3: One division "of equipment - with the associated piping, water sources, power supplies, controls, and instrumentation - that provides the capability to perform the functions (e.g., reactivity control, decay heat removal, process monitoring) that are necessary to achieve and maintain hot shutdown for a minimum of 8 hours from the time of reactor trip should be protected as vital. In addition, the major components of the reactor coolant makeup system and associated support equipment necessary to achieve this goal should be protected as vital."

    - Assumption 4: "The control room and any remote locations from which vital equipment can be controlled or disabled (e.g., remote shutdown panels, motor control centers, circuit breakers, local control stations) should be protected as vital area."

    - Assumption 5: "Only reactor power modes of power operation (Mode 1) and hot standby (Mode 3) need be considered as long as all equipment designated as vital for power operation is maintained as vital in other modes. Because secondary side cooling is disrupted in Mode 6 during refueling operations, Mode 6 is included. The safety-related system for heat removal required during secondary side isolation is considered in identifying vital equipment."

    - Assumption 6: "Offsite power is unavailable."

    - Assumption 7: "Random failures do not occur simultaneously with an act of radiological sabotage. However, the saboteur can take advantage of the unavailability of equipment during maintenance. Therefore, whenever any components or systems normally protected as vital are inoperable for any period of time, appropriate compensatory measures (e.g., stationing guards at alternate locations) must be taken to maintain the capability to reach hot shutdown."

    - Assumption 8: "Breaks in multiple main steam lines that cannot be isolated lead to 10 CFR Part 100 [10 CFR 52.47(a)(2)] releases."

    - Assumption 9: "Cable runs in trays and conduit need not be protected as vital unless cables necessary for safe-shutdown capability are individually identifiable and the identification is reasonably accessible. However, cable terminals or junctions and areas (e.g., cable spreading rooms) through which large numbers of cables pass, must be protected."

- Assumption 10: “Saboteurs may use explosives in amounts they can carry.”
- Assumption 11: “No credit is specified for equipment not located in vital areas.”
- Assumption 12: “Spent fuel pool should be protected as vital to prevent sabotage to the pool from resulting in a 10 CFR Part 100 [10 CFR 52.47(a)(2)] release.”
- Assumption 13: “Backup supporting power supply of the CAS is essential for continuous operation of CAS in the event of loss of normal power.”

- The applicant states the following additional assumptions in TR ANP-10295, Appendix A, Section A.2, for the plant systems and configurations:
  - Assumption 14: “Reactor coolant pressure boundary (RCPB) remains intact.”
  - Assumption 15: “Secondary pressure boundary remains intact.”
  - Assumption 16: “No random single failure.”
  - Assumption 17: “Reactor trip, loss of offsite power, and reactor coolant pump (RCP) trip occur or are initiated at time = 0 seconds.”
  - Assumption 18: “The plant stable state is hot shutdown (Mode 4) for 8 hours (minimum).”
- The applicant further states the following:
  - “Reactor Coolant Pressure Boundary – The RCPB is assumed to remain intact based on isolating the Reactor Building at the containment isolation valves and RCPB interface valves with other systems. The majority of the containment isolation valves are inside the vital structures. Those isolation valves outside the vital structures are required to be operated will be identified. The flow paths that are necessary to support reactivity control, core decay heat removal, reactor coolant makeup, and reactor coolant pressure control will remain in service. If the secondary pressure boundary remains intact, equipment to mitigate the effects of a steam or feed line break is not required to be protected.”
  - “Secondary Pressure Boundary – The secondary pressure boundary is assumed to remain intact. The majority of the secondary pressure boundary is located within the vital structures. Feedwater (FW) isolation valves and steam generator blowdown isolation valves are located in vital structures. The steam line isolation valves are located outside vital structures in the main steam and feedwater valve rooms. If the secondary pressure boundary remains intact, equipment to mitigate the effects of multiple steam line failures are not required to be protected. Releases in excess of 10 CFR Part 100 [10 CFR 52.47(a)(2)] [guidelines] will be prevented.”
  - “Random Single Failures – Random single failures are not required to be assumed. Therefore, redundant equipment is not required to be available to

mitigate a single failure. It is assumed that all active components will work properly if they are in a protected area."

- "Loss of Offsite Power – The assumption is that at the initiation of the event, the reactor will be tripped, the reactor coolant pumps will be tripped, and offsite power is lost. NUREG-1178 requires [sic] the assumption of a LOOP as part of the radiological sabotage event. The basis for this assumption is the difficulty in protecting the electrical distribution components outside the site controlled area. If these conditions do not occur at the initiation of the event, it is expected that the operators will manually perform these actions to place the plant in a known stable state at the initiation of the event. No design-basis accidents or events are assumed at the initiation of the scenario. However, consideration was specified for removing one safety-related electrical division from service (e.g., emergency diesel generator maintenance)."

- "Plant Mode – NUREG-1178 identifies hot shutdown as the applicable stable plant mode required for a minimum of 8 hours. Hot shutdown is defined as Mode 4 and correlates to reactor coolant (RC) temperature as being between 93.3 °C (200 °F) and 176.7 °C (350 °F). This mode will be considered the safe-shutdown condition for the purposes of this document."

- "Containment Isolation – Based on Assumption 2, no credit is specified for the protective or mitigating capabilities of the pressure vessel or the containment. Therefore, containment isolation is not considered to be a requirement for the radiological sabotage scenario."

Vital Equipment List

The applicant identifies a list of vital equipment in TR ANP-10295, Appendix A, "Vital Equipment List," Section A.4. The specific vital equipment (i.e., structure, system, and component (SSC)) and its locations are considered safeguards information, and are protected in accordance with 10 CFR 73.21.

The applicant indicates that equipment selected for protection (i.e., as vital equipment) is based on meeting the safety-functions identified in TR ANP-10295, Appendix A, Section A.1 (i.e., functions associated with reaching and maintaining a safe-shutdown conditions, reactivity control, reactor coolant make-up, reactor coolant system pressure control, decay heat removal, and process monitoring).

The applicant states that the "U.S. EPR is designed to cope with events and reach hot shutdown with a single division of safety-related equipment performing its accident mitigation function. There are cases in PRA analyses or beyond-design-basis scenarios where the initial assumptions result in no divisions remaining functional. In those cases, multiple divisions of other components may be required." Also, safety-related divisions were selected as the equipment divisions requiring protection. "For the most part, the divisions are redundant to each other and allow for extended emergency diesel generator maintenance on one division while maintaining a protected division. This selection provides the most flexibility based on plant arrangement. Again, selected equipment in other areas will require protection and will be designated as vital."

Relation of Probabilistic Risk Assessment to Vital Equipment

The applicant stated that the "U.S. EPR standard design process included a risk assessment of the design to optimize the plant with respect to safety." The "results of the PRA analysis are used in the selection of equipment or systems as potential vital equipment and subsequent determination of target sets and individual target set components." The assumptions used to incorporate PRA-related sequences into identifying the vital equipment are presented in TR ANP-10295, Appendix A, Section A.5.

The applicant's key assumptions and consideration of PRA insights are the following:

- PRA Insight and Assumption 1: "Certain immediate operator actions are taken by procedure immediately upon confirmation of adversary penetration of the protected area. These actions are taken to preclude certain failure states that may be discussed in the PRA. The equipment to be operated is included as vital equipment. These immediate actions are included in TR ANP-10295, Appendix C, "Operator Actions Benefiting Security."

- PRA Insight and Assumption 2: "Probabilistic failures to act on proceduralized operator actions assumed in the PRA are synonymous with random failures that are excluded from consideration by Assumption 7 from NUREG-1178 (Reference 5). Operator failures to act are, for the purposes of vital area analysis, based solely on adversary intervention (through use of lethal force or causing life threatening environmental conditions (e.g., fire, smoke, steam, floods, release of hazardous chemicals)) at the location of the operator action or along the available operator paths of travel."

- PRA Insight and Assumption 3: "Probabilistic failures because of natural events (e.g., earthquakes, tornados) assumed in the PRA are synonymous with random failures that are excluded from consideration by Assumption 7 from NUREG-1178 (Reference 5)."

- PRA Insight and Assumption 4: "Probabilistic equipment failure or piping failure (e.g., probability of a piece of equipment failing to start upon demand or pipe rupture resulting in loss of coolant events) assumed in the PRA are synonymous with random failures that are excluded from consideration by Assumption 7 from NUREG-1178 (Reference 5). Any loss of equipment would require physical adversary intervention at the point of damage."

- PRA Insight and Assumption 5: "PRA common cause failures are excluded from consideration, because they must fall into one of two states, each precludes substantial negative impact on the health and safety of the public."

- PRA Insight and Assumption 6: "Spurious activations assumed in the PRA are synonymous with random failures that are excluded from consideration by Assumption 7 from NUREG-1178. Any equipment state change would require physical adversary intervention with the equipment or control system."

- PRA Insight and Assumption 7: "The U.S. EPR is a four safety-division design. It is generically assumed that one division is in maintenance outage, one division

fails to actuate, and two divisions are available and operational to perform their intended safety function. Therefore, all four trains or divisions of required systems will be specified as vital equipment."

- PRA Insight and Assumption 8: "Piping that connects pieces of equipment specified as vital equipment is also generically considered vital equipment to the extent that the portion of the system pressure boundary is required to perform the intended function. Portions of a piping system that is normally isolated (e.g., by valves, check valves), and whose failure would not significantly affect the pressure boundary of the safety-related system alignment are not considered as vital."

- PRA Insight and Assumption 9: "Portions of a piping system isolated by immediate operator action as found in TR ANP-10295, Appendix C, that, after isolation, would not affect the pressure boundary of the safety-related alignment are not considered as vital."

- PRA Insight and Assumption 10: "Portions of electrical systems isolated by immediate operator action as found in TR ANP-10295, Appendix C, that, after isolation, would not affect the availability of required power to safety-related equipment are not considered as vital."

- PRA Insight and Assumption 11: "Electrical systems protected from remote shorts/failures by protective relays are not considered as vital (e.g., damage to remote portions would not affect the availability of required power to safety-related equipment)."

- PRA Insight and Assumption 12: "Flooding in the Annulus which may also impact mechanical equipment in Safeguard Buildings constitutes approximately 10 percent of the overall risk. Security personnel and features are in place to protect those onsite systems utilized to prevent challenges to these systems by adversarial actions. No onsite actions can prevent the LOOP event because of offsite exposure of transmission lines, but the onsite mitigation systems are protected from adversarial action by defensive personnel located in bullet resistant enclosures (BREs) in the vicinity."

- PRA Insight and Assumption 13: "Security personnel are located to prevent adversarial access to the vital areas which are associated with PRA flooding and fire-related risk. The structures that are not considered vital are defended by security personnel to deny access."

In responses to requests for additional information, RAI 42 and 92, submitted December 9, 2008, and December 5, 2008, respectively, the applicant provided the following clarification for determining vital equipment and the considerations of PRA and other risk assessments for determining vital equipment:

- The loss of offsite power was considered in the applicant's development of vital equipment. "Loss of coolant accidents were considered and addressed by identification of structures, systems, and components required for protecting the reactor coolant system pressure boundary. Safety-related cooling of the

RCP thermal barrier is provided by the component cooling water system." The applicant stated that "a loss of coolant accident (LOCA) by means of the RCP seal was not considered."

- "The identification and listing of vital equipment include active components of various systems whose operations are needed to provide safety functions. Some systems are generically treated as passive components, similar to piping, and therefore are not specifically listed. Piping and other passive components that connect pieces of vital equipment are also generically treated as vital equipment where they comprise a portion of the system pressure boundary that is required to perform the intended safety functions. Portions of piping systems that are normally isolated by valves (e.g., pressure relief valves, check valves) are not considered as components of vital equipment."

- "Similar to passive components, the support equipment and systems for active components of various systems whose manipulation are required for operations of that mitigation system are generically treated as integral to the active component operations, and they are not specifically listed. Heating, ventilation, and air conditioning include component coolers or room coolers for maintaining function of the systems and environment for personnel. The active components of support systems required for maintaining safety functions are discussed and included in the Vital Equipment List."

- "Auxiliaries (e.g., power, control circuitry, ventilation, cooling water) are considered integral parts of the listed vital equipment to the extent necessary to support the completion of the vital functions. The support systems are included in the Vital Equipment List. Trip sensors, cabinet housing protective systems, diverse scram systems, pressures retaining components, water sources, valves, pumps, power supplies, and control systems and other related protective systems equipment integral to the safety function of the listed vital equipment are considered vital to the extent necessary to support the completion of the vital equipment's function."

- "The Vital Equipment List provides the active components of various systems whose manipulation are necessary for operation of that mitigating system. Support equipment and systems are generically treated as integral to that component's operation; therefore, they are not specifically listed. Heating, ventilation and air conditioning (HVAC) includes the component cooler or room cooler required to maintain functionality of key components or to provide suitable environmental conditions for required personnel for up to 30 days after the event. The HVAC for a specific division or structure is comprised of the safety chilled water system and maintenance HVAC systems specific to that structure. These are supported by the four division-specific component cooling water systems which in turn are supported by the four division-specific emergency service water systems. The active components of these supporting systems meeting the assumptions in TR ANP-10295, Appendix A, Section A.4 are included in the Vital Equipment List."

- The U.S. EPR incorporates a four safety-division design. The applicant's assumptions are that one train may be in maintenance outage, one train fails to

actuate due a malevolent act, and two divisions are available and operational to perform their intended safety function. The design considered inter-independencies between trains, and the applicant indicated that in the cases where a component fails and the malevolent act impacts or damages two trains, one train would remain available to perform required and intended safety functions. The impact of a single event affecting two divisions is addressed by design of the U.S. EPR to maintain available one fully functional train to provide required safety functions. In addition, the applicant also credits operation actions to interrupt sequence progression and prevent fuel damage; availability of engineered and administrative controls for the physical protection system of the plant, as described in TR ANP-10295, Appendix C, to interdict and neutralize adversaries from performing malevolent acts; and design of equipment to fail in a safe configuration.

- The applicant assumed that piping and control cables in the plant are generally not labeled as to system or purpose. Generic unlabeled piping is not quickly or easily identified by persons not intimately familiar with the facility. The applicant stated that this conformed to guidance in NUREG-1178, on the classification of unlabeled electrical cabling that connects vital electrical equipment.

- The applicant applied NUREG-1178, Assumption 2, in developing the Vital Equipment List, and the containment isolation valves are assumed not to have isolated the system. However, the containment isolation valves that meet the definition of vital equipment are included as vital equipment.

- "All equipment contained within the identified vital areas is not vital equipment. All vital equipment is in a vital area, and all equipment necessary to support the function of the vital equipment is in a vital area. However, there are components that do not meet the definition of vital equipment that are also located in vital areas. The Vital Equipment List contains the list of equipment whose active function is required to prevent damage to irradiated fuel. Passive equipment that supports the operation of the listed vital equipment (e.g., piping, manual valves, pressure relief valves, check valves, control cable, power cables, cable trays, structures) are included in vital areas."

- The applicant stated that "operator actions may be or are taken immediately upon confirmation of adversary penetration of the plant protected area. These actions, normal, abnormal, or emergency operating procedures are taken to preclude certain failure states, which may or may not be discussed in probability risk assessment. The equipment to be operated is included as vital equipment. The immediate operator actions and the associated vital equipment are described in TR ANP-10295, Appendix C. Operator failures to act are, for the purpose of the vital area analysis, based solely on adversary intervention at the location of the operator actions."

- "Internal flooding is a random failure and is not considered in determination of vital equipment per NUREG-1178. The PRA flood scenarios specified in FSAR Tier 2, Table 19.1-41, "U.S. EPR Important Cutsets - Level 1 Flooding," were evaluated to verify that, based on the assumptions in TR ANP-10295, Appendix A, Section A.5 and the flooding scenarios specified in FSAR Tier 2,

Table 19.1-41, they were either bounded by generic vital areas (those listed as vital areas without specific equipment being identified), were invalidated by immediate operator actions specified in TR ANP-10295, Appendix C, or were bounded by equipment on the Vital Equipment List. In addition, the U.S. EPR is a four safety-division design. It is generically assumed that at least two divisions are available and operational to perform their intended safety function. In the case of failure to automatically swap divisions, manual operator action in accordance with normal, abnormal, or emergency operating procedures could correct the failure of the system to automatically swap divisions and manually restore division function. Emergency feedwater (EFW) piping was evaluated accordingly to determine whether selected piping is required to be identified as vital equipment."

- "System depressurization is accomplished by the vital equipment specified. Fires and primary feed and bleed were excluded under Assumption 7 of NUREG-1178 on random failures. PRA fire scenarios (FSAR Tier 2, Table 19.1-66, "U.S. EPR Important Cutset Groups – Level 1 Fire Events") were evaluated to ensure that, specified the assumptions outlined in the applicant's December 5, 2008, response to RAI 92, Question 13.06-21, the fire scenarios specified in FSAR Tier 2, Table 19.1-66 were either bounded by generic vital areas (those listed as vital areas without specific equipment being identified), were invalidated by immediate operator actions specified in TR ANP-10295, Appendix C, or were bounded by equipment on the Vital Equipment List."

The staff has determined the following:

- The staff has determined that the applicant applied the NUREG-1178 assumptions, which are not specifically intended for identifying vital equipment in accordance with definitions of 10 CFR 73.2. The study documented in NUREG-1178 was an attempt, in the pre-9/11 environment, by the staff to establish an approach for determining what safety functions and associated SSCs should be protected against the DBT for radiological sabotage in the 1980s. For example, Assumptions Nos. 3, 5, and 9 in NUREG-1178 are contrary to regulation of 10 CFR 73.2 that defines vital equipment. The remaining assumptions are related to systems and plant configurations such as core damage, protection of control room, unavailability of off-site power, conditions leading to 10 CFR Part 100 release, use of explosives by saboteurs in the pre-9/11 environment, equipment not located in vital areas, protection of spent fuel pool, backup power, and operator or adversarial actions. The PRA assumptions are also related to descriptions of systems or plant configurations (i.e., system remains intact, single failure, reactor trip, plant stable state, random single failures, loss of offsite power, containment isolation) that do not provide assurance that the process applying the stated assumptions would result in identifying a complete and accurate list of vital equipment as defined by 10 CFR 73.2.

- The staff has determined that the applicant's process for identifying a complete and accurate list of vital equipment did not adequately address the following:

- The identification of vital equipment based on the nuclear power reactor plant design and the structures, systems, and components that have been designated as safety-related.

- Vital equipment includes all reactor designed SSCs providing safety functions that prevent or protect against the release of radioactive material that could endanger the public health and safety by exposure to radiation, as stated in 10 CFR 73.2.

- All reactor SSCs designed to function to prevent release of radioactive material that would exceed the radiological exposure stated in 10 CFR 52.47(a)(2), are identified as vital equipment. In addition, all safety-related SSCs that function to protect against radiological exposure exceeding the threshold of 10 CFR 52.47(a)(2), after the loss of SSCs that prevent the release of radioactive material, are also identified as vital equipment, in accordance with 10 CFR 73.2.

- Vital equipment, in accordance with 10 CFR 73.2, including "any equipment, system, device, or material," for all modes of nuclear operations (i.e., power operations, hot stand-by, cold shutdown, refueling) is identified.

- All designed reactor SSCs in all redundant safety divisions to function to prevent radiological release are identified as vital equipment.

- All equipment, systems, devices, or materials (i.e., supporting systems) that are relied on for control or motor forces (e.g., control systems, digital signals, electrical power, mechanical, compressed air, water, etc.) and function to prevent radiological release and protect against radiological exposure are identified as vital equipment (i.e., in accordance with the 10 CFR 73.2 definition that any equipment, system, device or material, the failure, destruction, or release of which could indirectly endanger public health and safety is vital equipment).

In view of the foregoing, the staff determined that the applicant's process for identifying vital equipment, did not result in a complete and accurate list of such equipment. Since the list of vital equipment is incomplete and inaccurate, the applicant is unable to meet the requirements of 10 CFR 73.55(e)(9)(i), which states, "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."

The staff has identified the concerns of applying the assumptions identified in NUREG-1178 as acceptable regulatory guidance in RAI 246. RAI 246 includes a number of questions on the process and assumptions for identifying a complete and accurate list of vital equipment in RAI 246, Questions 13.06-83 through 13.06-86, and Questions 13.06-105, through 13.06-119. RAI 246 follows up on previously issued RAI 92, which initially raised the staff concerns regarding the NUREG-1178 assumptions (i.e., RAI 92, Questions 13.06-09 through 13.06-19 and Questions 13.06-21 through 13.06-25) and the potential for a less than adequate identification of a complete and accurate list of vital equipment for the U.S. EPR standard design.

The staff has determined that the applicant's process did not provide adequate assurance for identifying a complete and accurate list of vital equipment as defined by 10 CFR 73.2. The staff

concludes that the regulatory significance is that the applicant cannot demonstrate that it has identified all equipment that is considered vital in accordance with 10 CFF 73.2. As a result of inadequacy of a process and results, the applicant cannot demonstrate that all vital equipment for the U.S. EPR standard design are located within vital areas in accordance with requirements of 10 CFR 73.55(e)(9)(i). 10 CFR 73.55(e)(9)(i) requires 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." As a result, the applicant has not established an adequate process to identify all vital equipment that will be located in vital areas in accordance with NRC regulation.

The staff has determined that the TR ANP-10295, Appendix A, Section A.4 listing of vital equipment based on stated assumptions is not complete or accurate. Therefore, the staff requested that the applicant provide a complete and accurate list of vital equipment for the U.S. EPR standard design in accordance with 10 CFR 73.2. **RAI 425, Question 13.06.02-1, which is associated with the above request, is being tracked as an open item**.

13.6.4.2.2 Vital Areas

The requirements of 10 CFR 73.55(e)(9)(i) state 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." The applicant identified in TR ANP-10295, Section 1, the vital areas for the U.S. EPR standard design. The U.S. EPR standard design vital areas consist of the various structural boundaries of the Nuclear Island and structures indicated on the footprint of the U.S. EPR standard design.

The applicant stated that the vital areas are developed from areas containing the safety-related systems and components identified on the Vital Equipment List and others areas required to be located in vital areas, such as CAS, SAS, and security secondary power supply, as stated in 10 CFR Part 73.

The applicant determined, on the basis of diverse locations of safety-related equipment that are considered vital, the building perimeters that bound the vital equipment are identified as boundaries of the vital areas. The applicant indicates that the design configurations of vital structures are considered and provide for restriction of access to buildings and limited access pathways between vital structures, which enhance physical protection. The specific structures boundaries that form the vital areas are identified in TR ANP-10295, Figures 1-1, "Vital Area Perimeter," and Figure 1-2, "Vital Islands Within Nuclear Island." The specific listing of structures that are vital areas is protected as SGI and is intentionally not reproduced in this report. The detailed information of the vital areas is considered SGI and is protected in accordance with requirements of 10 CFR 73.21.

The applicant describes the following design, performance, and assumptions for the engineered physical protection systems or features credited for the protection of the vital areas:

- Unoccupied vital areas entry/exits are locked and alarmed with intrusion detection systems that annunciate at the plant security alarm stations.

- The vital area boundaries are separated from the PA boundary by an isolation zone. The PA boundary is separated from the identified selected vital areas

(VAs) by a distance, as indicated in TR ANP-10295, which allows for sufficient time for security responders to engage adversaries prior to reaching the exterior of a vital structure.

- All openings exceeding a standard opening too small for passage of an individual, as stated in TR ANP-10295, will be provided with engineered systems or features that delay, deny, control, detect, or monitor unauthorized access.

- All ventilation openings will be designed, as described in TR ANP-10295, above grade, and access controlled and exterior equipment doors are sized to equivalent thickness of the vital structure wall. External equipment hatches will be designed to provide adequate blast protection. The remaining exterior doors will be hardened to provide substantial resistance to penetrations with delay performance as stated in TR ANP-10295, Section 7, "Delay Features."

- The applicant also stated that the "design of the standard U.S. EPR includes minimizing entry points that create physical configuration that funnels externally and internally of the vital island and vital structure that adversaries must transit to gain access to entry points." [sic] The applicant stated that "the design to minimize the number of entry points into vital areas was evaluated in FSAR Tier 2, Section 9.5.1, "Fire Protection System," and Appendix 9A, "Fire Protection Analysis," for fire protection and life safety to address potential safety/security interface concerns." Additional details of configurations are described in TR ANP-10295.

- Two-way communication for security response is provided by the security radio system. The capability is provided for command and control from alarm stations to direct defenders even when radio is unavailable. To accomplish this, alternative means of communications from the CAS and SAS do not rely on wireless communications. Surveillance systems are available for observation of adversary movement, as described in TR ANP-10295, Section 8.2. The design criteria for the security communication system are to be provided by means of COL Information Item No. 13.06-03 by the COL applicant in its site-specific Security Assessment.

- "Emergency exits are configured to provide a substantial delay to external penetration. This is accomplished with multiple layers of engineered delay features (e.g., by use of Government Services Administration (GSA) vault doors, as specific in TR ANP-10295). During normal operations, both normal and emergency exits are available for emergency egress, even with the loss of primary and backup security power, but can be made unavailable for ingress or egress during periods of hostile action."

- The TR ANP-10295 provides plan and section views to graphically represent the boundaries of vital areas of the U.S. EPR standard design. The applicant stated that "throughout the design certification process, the applicant will periodically review, and if necessary, update TR ANP-10295 to maintain consistency with other configuration information provided."

The staff has determined the following:

The staff has determined that the applicant has identified in TR ANP-10295, Section 1, Figures 1-1 and 1-2, the areas designated as vital areas for the U.S. EPR standard design. The results of the applicant evaluation and identification of the vital areas for the U.S. EPR standard design are documented in TR ANP-10295, which is referenced by FSAR Tier 2, Section 13.6. The U.S. EPR standard design vital areas consist of the various structural boundaries of the Nuclear Island and structures indicated on the footprint of the U.S. EPR standard design.

The staff has determined that the applicant has adequately addressed the requirements of 10 CFR 73.55(e)(9)(v) by design and designation of vital areas that include the reactor control room, spent fuel pool, central alarm station, and secondary alarm station, in accordance with 10 CFR 73.55(i)(4)(iii). In addition, the applicant has also adequately addressed requirements that secondary power supply systems for alarm annunciation equipment and the secondary power supply systems for non-portable communications equipment, in accordance with 10 CFR 73.55(i)(4)(vi), are located within vital areas.

The staff concludes that the applicant has adequately described the design, performance, and assumptions for the engineered physical protection systems credited for the protection of the vital areas. Specifically, TR ANP-10295 describes: Design requirements, physical protection systems, and configuration for the separation from the protected area; control of normal access and protection of emergency exits to detect and delay unauthorized access; physical barrier systems for protection of all penetrations into the vital area; detection surveillance, assessment and communications systems for detection of unauthorized access and initiating security response; and measures to minimize points of entry and pathways into each vital area that limit accessibility to separate safety divisions (i.e., vital equipment) and channel adversaries to locations of pre-deployed security responders).

In RAI 246, Question 13.06-83, the staff requested that the applicant provide a complete and accurate list of vital equipment for the U.S. EPR standard design. The staff could not determine: (a) Whether designated vital areas currently identified contain all vital equipment for the U.S. EPR standard design; (b) whether vital equipment not currently identified is located outside of the areas currently designated as vital areas; and (c) whether the applicant has appropriately identified for Commission consideration any vital equipment that will be located outside of designated vital areas. As a result, the staff issued a follow-up RAI 425, Question 13.06.02-2, requesting that the applicant meet the requirements of 10 CFR 73.55(e)(9)(i) and that the designated vital areas include all the vital equipment as defined by 10 CFR 73.2. **RAI 425, Question 13.06.02-2 is being tracked as an open item**.

13.6.4.2.3 Target Sets

TR ANP-10295, Revision 1, Appendix F, “Target Sets,” dated October 28, 2009, identifies the target sets based on the U.S. EPR standard design. The applicant indicates that target sets consist of reactor structures, systems, and components and operator actions and associated equipment that must be protected by the COL applicant protective strategy (i.e., physical protection engineered and administrative controls) to demonstrate adequate protection of the reactor plant and operations against the DBT, including active and passive insiders, for radiological sabotage. In TR ANP-10295, Section 11, “Target Sets,” the applicant states the following for determination of target sets based on the U.S. EPR standard design and certification:

- Target Sets are not considered by AREVA to be in the scope of the U.S. EPR design certification. Target Sets are an integral component of the security drills and exercise operational program and require updating and maintenance over the entire lifetime of the license. Target Sets also require a comprehensive evaluation of the site, including certain features to be determined by the COL applicant (e.g., supplemental systems or operator actions credited beyond those credited in the design certification evaluation). It is not anticipated that the COL applicant supplements would reduce the number of Target Sets or remove any of the items within the Target Sets. However, Target Sets are beneficial in establishing an overall defensive strategy during the design certification activities. Therefore, Target Sets were developed to assist AREVA personnel in evaluating the defensibility of the site and to assist AREVA personnel in evaluating optimal physical locations for defensive positions.

- TR ANP-10295, Appendix F contains a description of target sets and the method of their development which conforms to Nuclear Energy Institute (NEI) 03-11, "Guidance for the Preparation and Conduct of Force-on-Force Exercises." For these reasons, target sets have been included in TR ANP-10295, Appendix F, and they are used in the development of the U.S. EPR security features. These target sets serve as the basis for the COL applicant development of the site-specific target sets. The COL applicant may incorporate these target sets as written by reference or may modify these targets sets as additional site-specific details require.

The applicant also states that, "after licensure, the COL Holder is solely responsible for Target Sets for the site."

A summary of the process described in TR ANP-10295 for determining target sets is the following:

- The key assumptions related to the method for development, validation and revalidation of target sets in TR ANP-10295, Appendix F, Section F.5, "Target Identification," include: (a) The target sets provide a tool for developing the site-specific protective strategy; (b) target set development considers the consequences of groups of structures, systems, and components not being functional; (c) regardless of whether the loss of function is caused by a broken component or attempted radiological sabotage, target set analysis may take advantage of risk insights developed from comprehensive plant reviews; (d) the target sets are developed using an expert panel with insights from the Safe-shutdown Equipment List (SSEL) and the PRA analyses; and (e) the target sets are applicable to all operational modes.

- The process calls for an expert panel to identify the SSCs to be protected. The expert panel includes members with expertise in security and key areas of plant design and operations. Other disciplines (e.g., systems engineering, maintenance, regulatory affairs, licensing, emergency response planning, and training) are considered where the expertise can aid target set development or revision. Some members of the panel should be able to review the target sets from the adversary view.

- "The performance criteria used in developing a site's target sets are fully documented as part of the process. The criteria will provide for some margin of protection of public health and safety by preventing core damage that would result in a significant radiological release. Some of the criteria will be provided to the expert panel as a starting point for their work. For example, preventing significant core damage is a key performance criterion to be used in the force-on-force process. The panel may develop other criteria as part of the project."

The applicant provides examples of what was considered in developing performance criteria used at the sites including:

- Loss of offsite power may occur prior to, or concurrent with, attempts at radiological sabotage.

- Different divisions of redundant systems are to be considered separately when they are located in different rooms or geographical areas.

- Cable runs in trays and conduit need not be considered if identification is not reasonable in a short period of time.

- All site systems are available. Random failures do not occur simultaneously with an act of radiological sabotage.

- Alternate equipment configuration is available within the time frame that it would be needed to function to mitigate conditions.

- "NUREG-1178 provides insights on things to consider in developing target set criteria. Because NUREG-1178 focuses on vital areas, not all of the assumptions are applicable when considering elements of target sets. For example, items outside vital areas but inside the protected area and under the site's control can be considered in developing target sets."

In TR ANP-10295, Appendix F, Section F.5, the applicant provides a list of structures, systems, and components that support the COL applicant's ability to meet the selected performance criteria for developing target sets. The applicant describes the following five steps of the process:

- The applicant states that the first step for identifying target sets is the establishment of an expert panel that would identify the potential of radiological source terms that could result in consequences that exceed 10 CFR Part 100 guidelines for both operating and shutdown conditions. An example that meets potential of radiological source terms is the reactor core, as required by 10 CFR Part 73, and "analyses of other areas (e.g., the spent fuel pool) needs to determine whether there is sufficient radiological source terms for the release to exceed limits."

- The second step in the process is to identify the barriers for preventing the release of radioactive material. The applicant states as an example that the process would identify the "reactor fuel cladding, reactor coolant system piping,

and containment integrity as barriers" that would be credited to contain and prevent the release of radioactive material.

- The third step is to identify the release paths and include as part of the evaluation, the safety/security significance related to loss of a specific target set.

- The fourth step in the process is for the expert panel to develop a list of SSCs, based on the U.S. EPR standard design, that affect barrier integrity or impact other performance indicators. The applicant states that "the objective is to identify all SSCs that can be used to mitigate the impact of loss of other equipment." Examples of SSCs that would be considered based on their safety-related functions are: "reactor coolant inventory sources (e.g., tanks, pools), power sources (e.g., electrical, steam), physical barriers (e.g., containment, system piping), equipment (e.g., pumps, fans), key plant personnel (credit for personnel action), and sufficient equipment that provides the capability to perform the functions that are necessary to achieve and maintain hot shutdown for a minimum of 8 hours."

- The final step in the process is to consider other non-safety-related systems, administrative controls (i.e., operators and procedures), and emergency responses that may be credited based on availability, including locations, that may contribute to mitigate the loss of barriers or provide alternatives for loss of safety-related functions.

The applicant provided some examples as to what would be considered as follows:

- The plant's normal and abnormal operating procedures (operator actions) and capabilities to mitigate failed conditions.

- The electrical support requirements for mitigating equipment, including alternating current (ac), direct current (dc), and instrument control power.

- The non-electrical support requirements for mitigating equipment, including equipment and room cooling, water sources, vulnerable pipe sections, and their locations.

- Emergency planning insight into plant vulnerabilities, potential mitigating activities, and the range of recovery actions that could be reasonably assumed to occur under conditions associated with postulated events.

- Operating alternatives for degraded plant conditions.

- Accident sequences and potential mitigating activities and the time frames that would be required for significant core damage to occur.

- For potential mitigating activities, security coordination and interface with operations.

- "Contingency plans for alternate equipment lineups and potential mitigating activities."

In TR ANP-10295, Appendix F, Section F.6, "Target Set Analysis," the applicant describes the next step in the process that evaluates or analyzes the relationships and dependence between systems. The applicants states that, "the targets identified from the previous steps shall be used to identify sets of multiple targets whose concurrent damage could prevent fulfilling a key requirement [sic] (e.g., core cooling). The expert panel organizes target sets that show the relationships and dependence between systems. This may be a listing of targets in prioritized logical format, or the target may be organized in a sabotage fault tree." The applicant states the following:

- A sabotage fault tree is a graphical, Boolean logic diagram, which identifies the combinations of target sabotage events that could lead to significant core damage. The sabotage fault tree is relatively simple and has been developed from a site-specific PRA.

- The targets are organized into common elements (e.g., location, power source, subsystem dependencies between the SSCs). When evaluating a specific system or component, the team should consider an adversary's ability to damage a system from remote geographical locations. Examples are as described in TR ANP-10295, Section F.6. The applicant indicated that the consideration of dependencies should be applied to each potential target and other criteria to include ease of access, the degree of probability for success, and the value of the target to plant shutdown.

- An example of four targets organized into 10 target sets is shown in TR ANP-10295, Appendix F, Table F-1, "Target Sets." In the example, there are four typical SSCs that will prevent significant core damage. All four of the SSCs must be rendered non-functional to complete the target set. Target set one (Column 1) demonstrates a successful target set, because the power is removed from three of the four SSCs, and the fourth is made non-functional by disabling the controls. A successful security strategy would be to prevent the adversaries from disabling at least one of the SSCs within each target set so it will remain available to cool the core. This example does not take into account any subsystem dependence.

The applicant stated that, "the matrix of Target Sets can be quite large and needs to be further refined to support a reasonable number of target sets to support the protective strategy. The physical location and access needs to be considered in this phase. If in the example shown above, the suction and discharge were in the same location as the equipment then the three could be combined as one element. Viewing the target sets from an adversary's vantage point can help in this refinement."

In TR ANP-10295, Appendix F, Table F-1, the applicant describes the results of applying the process described above for the U.S. EPR standard design target sets. The applicant restates that "Target Sets are not considered by AREVA to be in the scope of the U.S. EPR design certification. Target Sets require a comprehensive evaluation of the site, including certain features to be determined by the COL holder." The details of the target elements and target sets are SGI and/or security-related information and are withheld in accordance with 10 CFR 73.21 and 10 CFR 2.390.

The staff issued RAI 246, Questions 13.06-80, 13.06-81, 13.06-83, and 13.06-91 through 13.06-94 related to the process for identification and resulting target sets for the U.S. EPR standard design. In addition, the staff also issued RAI 246, Questions 13.06-82, 13.06-84 through 13.06-86, and 13.06-105 through 13.06-118 related to identifying a complete and accurate identification of vital equipment meeting requirement definition of 10 CFR 73.2. The staff identifies the need to confirm adequate responses for Questions 13.06-84 and 13.06-86. The remaining questions, identified above, are unresolved issues resulting in tracking of the staff request to provide a complete and accurate list of vital equipment as an open item.

On the basis that the applicant has stated that target sets are not within the scope of the design certification and will be further developed by a COL applicant referencing the U.S. EPR standard design, the unresolved issues related to the process for identification and resulting target sets for the U.S. EPR standard design will be a potential open item for a COL that incorporates reference the information on target set as currently provided in TR ANP-10295 for the U.S. EPR design.

The staff determined and concludes the following:

- The applicant states that, "Target Sets are not considered by AREVA NP to be in the scope of the U.S. EPR design certification." On the basis that the requirements of 10 CFR 73.55(f), "Target Sets," and 10 CFR 73.55(b)(3) that "the physical protection program must be design to prevent significant core damage and spent fuel sabotage" is programmatic in nature and/or cannot be addressed fully in the scope of the design certification, the staff determines that the applicant demarcation of the scope between the U.S. EPR design certification and that of a reference COL applicant as reasonable and adequate. The applicant has established a process to develop and identify target sets (i.e., a standard target sets based on the U.S. EPR standard design) to evaluate and consider defensibility of the site and evaluate optimal physical locations for defensive positions. The identified target sets serve as a basis for the COL applicant development of site-specific target sets. The applicant does not anticipate the COL applicant supplements would reduce that number of or remove any of the items within the standard target sets.

- The applicant's process for identifying target sets involves the establishment of a multi-discipline team that includes individuals knowledgeable on electrical and mechanical systems, security, emergency preparedness, operations, licensing, and engineering integration and involve five major steps. The staff concludes that the applicant process to establish a multi-discipline team to be reasonable and provide adequate assurance that appropriate subject matter experts are included in the determination of target sets. However, the staff identified unresolved issues that must be addressed for assumptions or criteria identified in TR ANP-10295, Appendix F, "Target Sets," as identified in RAI 246 and, if unresolved, must be addressed by the COL applicant referencing the U.S. EPR standard design.

- The applicant has identified standard target sets that describe the safety functions of a combination of equipment (i.e., safety-related and non-safety-related) that must be protected by a site protective strategy to prevent

significant core damage. The applicant also describes and identifies safety functions that must be protected for preventing the loss of spent fuel pool cooling.

The applicant identifies standard target sets by descriptions of safety functions that bound the systems (active and passive components), and supporting systems or equipment, including operator actions that may be relied on or are needed to achieve the stated safety functions. The staff identified unresolved issues for identification of complete and accurate target sets that must be protected against the DBT for radiological sabotage.

The staff concludes that the review of whether the applicant will meet the requirements of 10 CFR 73.55(f), "Target Sets," for a process of identifying target sets and whether the resulting target sets are adequate and are protected by a physical protection program designed to prevent significant core damage and spent fuel sabotage in accordance with performance requirements of 10 CFR 73.55(b)(3) are beyond the scope of the design certification. Compliance with these regulatory requirements must be addressed by the COL application referencing the U.S. EPR design.

13.6.4.2.4 Physical Protection System Assessment - Protective Strategy

The applicant states the U.S. EPR standard design incorporated a number of physical protection systems, components, or features to facilitate and enhance the implementation of physical protection of the U.S. EPR Nuclear Island and safety-significant structures, systems, and components. Physical protection systems, features, or configurations of vital island and structures that will be incorporated in the final design of the U.S. EPR standard design, within the scope of certification, include the following:

- Minimizing the number of access points into vital areas and between vital areas and structures
- Layout of security force protection of access points
- Layout of structures and location of security posts to minimize blind spots and enhance monitoring and plant layout to enhance defensive fighting positions (e.g., protection from adversary suppressive fire and fields of fire)
- Provisions for a minimum set of security posts needed to protect access to vital areas
- Provisions for passive and active delays and access denial systems
- Protection of the central and secondary alarm stations
- Design features for security monitoring vital areas and access to vital areas and security zones
- Physical protection of doors and penetrations of credited barriers for delay (including reactor containment, such as emergency core cooling system piping into Annulus, HVAC penetrations, etc.)

- Configurations and hardening of interior and exterior doors for access, delay, and protection against explosives
- Provisions for primary and backup power supply (e.g., uninterruptible power supply and emergency generators) for security-significant systems
- Provisions for reliable plant security lighting
- Protection of digital security systems and protection of cable routing and redundancy
- Provisions for local monitoring capabilities at security posts
- Consideration of human/machine interface of security design features
- Provisions in facility/room environment to enhance personnel attentiveness
- Provisions for mitigating insider threat (e.g., separation and redundancy of safety systems, tamper and abnormal condition alarms, facility layout for access control, active and passive barriers, interior intrusion alarms, monitoring, and interior cameras)
- Provision for personnel protection or survivability against hazards, such as radiological, chemicals, and fire, for CAS, SAS, defensive posts, and ready rooms (e.g., high-efficiency particulate air (HEPA) filtration, recirculation and fresh air supply, fire-rating, bullet resistant, differential pressures, room HVAC dampers, etc.)
- Provision for securing and permitting use of emergency exits
- Plant layout to protect against DBT explosive threats (i.e., standoff distances)

The applicant indicated that a security assessment was performed to determine how it would effectively protect the potential target sets of the U.S. EPR standard design. The security assessment, along with determining bases for the design and performance credited for physical protection systems (as stated above), resulted in a proposed standard for internal security defensive positions based on the vital island and vital structures that considered minimizing access points and pathways between structures. The standard locations of security defensive positions are described in TR ANP-10295, Appendix D, “Internal Defense Positions.” The figures in TR ANP-10295, Appendix D (Pages D-2 through D-12) identify the specific defensive positions at various elevations and locations within the vital island and vital structures that are a part of the U.S. EPR standard design.

In addition, the engineered barriers to delay adversaries are described in TR ANP-10295, Appendix E, “Internal Delay Features.” These engineered barriers also provide protection of security responders and facilitate security responses for postulated scenarios. The applicant indicated that it considered engineered delay systems that are available and applied for physical protection and control of access, both passive delays such as hardening of access or openings to provide passive delay and active delay or deployable systems. The engineered barriers and delay features for the U.S. EPR standard design are described on figures in TR ANP-10295,

Appendix E, “Internal Delay Features” (Pages E-3 through E-13). The applicant indicates that the design criteria for internal delay features will be described in the site-specific Security Assessment to address a COL information item.

The staff has determined the following:

- The applicant has considered needs for physical protection and provided enhancements of the vital island and vital structures for physical protection in the development of the standard footprint for the U.S. EPR standard design. Specifically, the applicant has minimized, in the U.S. EPR standard design, the number of access points into the vital island and structures and limited pathways between structure, which enhances and allows for implementing security response to contain and interdict adversaries along pathways and areas of the vital island and structures.

- The applicant has incorporated in the U.S. EPR standard design the locations and designs of defensive positions and engineered delay features, as described in TR ANP-10295, Appendix D and Appendix E for physical protection within the vital island and structures. The locations and design of defensive positions and delay features provide opportunities for interdiction along pathways which adversaries must travel to reach separated and redundant safety-related systems to initiate events leading to radiological sabotage, protect the security responders for interdiction of adversaries, and provides delay of adversaries to allow for deployment or re-deployment of security responders to the pre-determined defensive positions. However, the overall adequacy of a complete security plan applying these defensive positions and engineered delayed features for defense in-depth cannot be determined in design certification but will have to await a COL application that is required to describe how the COL applicant will protect the plant against the DBT.

- The applicant’s design and performance criteria for physical protection systems include the systems that will be credited for implementing the insider mitigation program. The physical protection systems that are relied on to implement the IMP within the vital island and vital structures, such as entry and exit access controls features; physical barriers; surveillance and assessment camera; intrusion, detection, and alarm systems, are described in the TR ANP-10295. The applicant has considered how these physical protection systems will be relied on and applied to prevent, control, and/or detect unauthorized access to vital areas for the protection against active and passive insiders.

Accordingly, the staff finds that the applicant has performed an adequate and reasonable assessment of physical configurations of the standard plant and the requirements for detection, assessment, communications, delay, and response for protection against the DBT of radiological sabotage and incorporated as part of the U.S. EPR standard design the physical protection systems and features, including designing of vital island and vital structures configurations, for enhancing and implementing physical protection and programs to comply, in part, with requirements of 10 CFR Part 73.

13.6.4.2.5 Security Computer Design Requirements and Cyber Security Program

The applicant states that the cyber security as required by 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks," is described in RG 5.71, Rev 0, "Cyber Security Programs for Nuclear Facilities," as "solely the responsibility of the COL Applicant." In TR ANP-10295, Section 5, the applicant provides explanatory information for use by the COL applicant in preparing the cyber security plan and procedures, and a general description of cyber security aspects of the U.S. EPR protection system is contained in TR ANP-10295, Appendix B, "Protection System Cyber Security." COL Information Item 13.6-4, identified in TR ANP-10295 (page ii) calls for a COL applicant referencing the U.S. EPR standard design to provide a cyber security plan meeting 10 CFR 73.54 in accordance with requirements of 10 CFR 52.79(a)(36)(iii). However, FSAR Tier 2, Table 1.8-2 which identifies COL information item numbers and description, did not include COL Information Item 13.6-4. In an October 3, 2008, response to RAI 78, Question 14.03.05-3, discussed in Section 13.4.4 of this report, the applicant committed to revise FSAR Tier 2, Table 1.8-2 to list COL Information Item 13.6-4. The staff finds this response acceptable. **RAI 78, Question 14.03.05-3 is being tracked as a confirmatory item**.

In addition, the applicant states the following for the design of security computer systems:

- The security computer system is a subsystem of the security system which interfaces with other security equipment and subsystems to satisfy functional requirements. The system supports the plant security staff by continuous access control and monitoring of all vital area doors and prompt reporting and permanent recording of all alarm points including intrusions, tampers, and trouble conditions. The plant security computer system provides alarm and event assessment functions for all security applications, access control, badging, personnel, security doors, intrusion detection system, complete biometric integration, and historical and reporting requirements. The security computer system also interfaces with closed circuit television system.

- The security computers are physically located within vital areas and access is restricted to authorized personnel. These are redundant security computers, spatially separated, independently powered by diverse security power subsystems and each are independently capable of providing required security functions. Software changes to the security computer system are restricted to authorized personnel.

- The security computer system is an isolated network and does not connect to any other plant systems, computer, or data networks. Security computer system connectivity utilizes an isolated dedicated communication network. Access to the security computer system network requires user authorization and is password protected.

The staff determined the following:

- The applicant has considered and commits to the physical and network control and isolation of the plant security computer systems to ensure the reliability and availability of physical protection systems for plant operations.

- The applicant indicates that the COL applicant referencing the U.S. EPR design is responsible for meeting the requirements of 10 CFR 73.54 for a cyber security program protecting digital computers and communication systems and networks. The staff determined that whether the applicant has met the requirements of 10 CFR 73.54 is beyond the scope of the design certification. Compliance with the regulatory requirements for an adequate cyber security program is to be reviewed as part of the technical review for a COL application referencing the U.S. EPR design.

- Standard Physical Protection Design Features

The applicant's TR ANP-10295 provides details of physical protection systems design and performance, along with technical bases and assumptions, for the U.S. EPR standard design. The details of the design and performance supplement and expand on the information described in FSAR Tier 1, Chapter 3, and provide design basis information for conducting inspections, tests, and analyses required for verifying construction, installation, and performance of physical protection systems stated in FSAR Tier 1, Table 3.1-1.

TR ANP-10295 describes the design and performance of the following physical protection systems within the scope of the design certification:

- Security power system (redundancy, separation, reliability, uninterruptible power supplies, critical security functions, and security power system)

- Bullet resistant walls, floors, and ceilings (main control room, central alarm station, and secondary alarm station)

- Vehicle barrier systems (Nuclear Island blast calculations, isolated vital structure blast calculations, SBODG Building, air-blast in leakage, external equipment doors, blast standoff distance)

- Defensive positions (internal and external)

- Delay features (vital area and internal delay features)

- Surveillance and monitoring (external, internal, certain areas outside of the protected area)

- Alarm stations (central and secondary alarm stations, redundancy, and separations)

- Insider mitigation (surveillance and margin analysis)

- Breaching of exterior walls (explosive and mechanical)

- Bullet resistant enclosures

- Interior security lighting

- Security electrical power supply

- Exterior security assessment model
- Operator actions benefiting security
- Target sets
- Security system test abstracts

The applicant describes the engineered systems and features the U.S. EPR standard design has incorporated, including configurations and layout, to provide, facilitate, or enhance capabilities to detect, assess, communicate, physically delay, and respond in order to protect the nuclear power plant against the DBT.

The specific details of design and performance of the physical protection systems and components that would reveal SGI or security-related information are protected in accordance with 10 CFR 73.21 and 10 CFR 2.390 and are not described in publicly available documents. The following sections of this safety evaluation describe the design and performance considerations for physical protection systems that have been incorporated as part of the U.S. EPR standard design.

13.6.4.2.6 Design Features for Detection and Assessment

The specific details of physical protection systems design basis, and assumptions are described in TR ANP-10295. In summary, the applicant describes the following design and performance credited for physical protection systems, including credit for the vital island and vital structures to provide physical protection functions:

13.6.4.2.6.1 Detection and Assessment

The applicant indicates that the U.S. EPR standard design includes a provision for installation of a security assessment system that consists of a combination of an electronic system and physical surveillance or observation capabilities from multiple locations, as described in TR ANP-10295. The applicant credits security personnel response to intrusion detection system alarms to survey their assigned zones in addition to the electronic assessment system. The assessment coverage includes all plant areas, as described in TR ANP-10295, using external and internal cameras, with assessment capabilities meeting the prescriptive regulatory requirements of 10 CFR 73.55(i)(1) through (i)(3) for detection and assessment and the assurance of detecting and assessing unauthorized access or attempted access.

The applicant states that the placement of specific location of assessment cameras to meet the design and intended assessment functions will be described by the COL applicant in the site-specific security assessment as part of the COL application (i.e., COL Information Item No. 13.6-03). The COL applicant is required to submit a security assessment that addresses the design and performance of the perimeter intrusion detection at the protected area, which is outside the scope of the U.S. EPR standard design certification.

In TR ANP-10295, Section 8, “Surveillance and Monitoring,” the applicant states that the external assessment system includes a camera system with video capabilities and is monitored from alarm stations and other locations. The design of the assessment system for external surveillance includes a combination of both fixed and pan-tilt-zoom cameras, and a mixture of low-light cameras and no-light cameras applying advanced detection technology. The

conceptual design of the external perimeter assessment system includes cameras that will be positioned to allow monitoring of the VA boundaries (e.g., assessments of adversary actions for security responses, monitoring of access to vital areas, etc.).

The applicant identifies as a design basis, the placement of external perimeter cameras to provide a redundant capability for the reliability and availability of monitoring for unauthorized activities. The design basis also establishes diversity, along with redundancy of coverage, of cameras using different technology to minimize the potential for single failure or conditions that would interfere with assessment performance capabilities. The cameras will be capable of monitoring from substantially different vantage points to minimize the value of adversary cover, and external camera pairs are powered from separate divisions of power to prevent a single power system failure from disabling the monitoring capabilities. The applicant states that the placement of external surveillance cameras is to be determined by the COL applicant in the site-specific security assessment as part of the COL application.

Internal Assessment System

The design of the internal assessment system includes cameras with capabilities required by 10 CFR 73.55(e)(9) and 10 CFR 73.55(i) for monitoring the vital island and vital structures, vital areas, and access points, including assessment based on intrusion detection. Interior lockdown doors are equipped with access controls designed to provide additional delay. The doors are locked and adversary access delays are protected as indicated in TR ANP-10295, Section 7. The design basis for the assessment system includes video capability that can be activated in detection mode to monitor interior areas within vital areas. The placement of internal surveillance cameras is described by the COL applicant in the site-specific security assessment as part of the COL application.

Areas Outside the Protected Area

Certain site-specific non-vital areas outside the protected area may also be protected by intrusion detection or video surveillance. These areas do not have an impact on the plant's ability to protect irradiated fuel, but would impact normal operations and longer term safety function capabilities. The assessment capabilities consist of monitoring these areas for security response upon alarm or detection of unauthorized access. The placement of the assessment cameras will be described by the COL applicant in the site-specific security assessment as part of the COL application.

Alarm Stations

The CAS located as described in TR ANP-10295, Section 9, "Alarm Stations," is protected from aircraft and blast effects of the design-basis threat vehicle bombs (as described in TR ANP-10295, Section 4.0). The location of the CAS is such that the interior cannot be observed from the PA perimeter, in accordance with requirement of 10 CFR 73.55(4)(ii). The design of the CAS will incorporate room ventilation capabilities of protection against postulated hazardous atmosphere conditions to assure continued operations. The CAS enclosure is bullet resistant to a specific Underwriter Laboratories (UL) standard, as described in TR ANP-10295, Section 3.1.

The SAS is located as described in TR ANP-10295, Section 9, "Alarm Stations," and protected from aircraft and blast effects of the design-basis threat vehicle bombs, as described in TR ANP-10295, Section 4.0. The location of the SAS is such that the interior of the SAS cannot

be observed from the PA perimeter, in accordance with the requirement of 10 CFR 73.55(4)(ii). The location of the SAS is spatially, separated by a non-adjacent building, from the CAS, to minimize the risk of common environmental effects (e.g., smoke) from affecting both facilities. The SAS enclosure is designed to meet regulatory requirements for bullet resistance to a UL standard, as described in TR ANP-10295, Section 3.2.

The design of alarm stations includes spatial separation and system redundancy to provide protection against a single act that could lead to loss of security functions of both the CAS and SAS. The CAS and SAS are provided with the equivalent level of physical protection by placement in separate hardened structures with separate ventilation systems. The applicant stated that the CAS and SAS have equivalent performance criteria (i.e., providing required and redundant security functions), but the physical layout may vary between the alarm stations.

Intrusion Detection System and Monitoring

The U.S. EPR standard design includes interior intrusion detection technology for activation of the internal assessment system and monitoring plant areas. The assessment system is partly provided for the purpose of implementing a physical protection system that is relied upon for insider mitigation. The applicant stated that the determination of plant areas for installation of intrusion detection will be at a minimum is based on the locations of systems and components important providing safety functions, as specified by conditions stated in ANP 10295, Section 10.1, “Surveillance.”

The vital areas or other critical or sensitive areas are monitored at multiple locations to detect unauthorized activities in the area. The applicant stated that the areas monitored included, but not limited to, rooms and equipment providing important safety functions, as described in ANP-10295, Section 10.1.

The detailed design addressing site-specific information for the assessment system is based on the conceptual design described in TR ANP-10295, will be provided by the COL applicant (i.e., Appendix D of the COL site-specific security assessment).

Security Power System

The power systems for the CAS and SAS are designed as equal and redundant divisions with reliable and separated power sources to prevent a single act from disabling critical functions. Each security power division will be designed with an independent diesel backup and supported UPS system. These features supporting the critical security functions will be placed in hardened structures that are separated, spatially remote from each other, and separated by ventilation and fire zones.

The secondary power supply will be from multiple sources as specified in FSAR Tier 2, Chapter 8, “Electric Power,” and capable of supplying power for at least 24 hours at a specified design load of physical security systems providing critical security functions. The critical security functions are powered by divisional uninterruptible power supplies to ensure continuity of functions during transfer from loss of normal power to diesel backup power. In FSAR Tier 2, Section 13.6, the applicant erroneously references that these power sources are described in FSAR Tier 2, Sections 2.5.1, “Basic Geologic and Seismic Information,” or 2.5.3, “Surface Faulting.” **RAI 425, Question 13.06.02-4 was issued to correct this reference and is being tracked as an open item**.

The applicant indicates that the design bases stated apply to providing the following critical functions: Evaluation of alarms and management of security response at the CAS and SAS; control of vital area access; PA and VA intrusion detection; exterior and interior security lighting; and security communications to defensive positions and local law enforcement authorities (LLEA). The physical protection systems that provide the stated critical functions, including internal and external surveillance cameras will be interconnected to the security power systems. The standard list of physical protection systems that will be designed with the reliability, separation, and redundancy of electrical power supply for the U.S. EPR design certification is identified in TR ANP-10295, Section 2.1.6.

The applicant determined the design for security lighting electrical loads in TR ANP-10295, Section 2.2. The design will be based on providing sufficient security power for an average external lighting level of 1 ft-candle (10.76 lux) to assure a 0.2 ft-candle (2.152 lux) lighting level may be maintained in all areas requiring lighting for detection, assessment, and response. Additional capacity will be provided for interior lighting for emergency egress and internal security response (i.e., defensive actions). The applicant indicates that it assumes a COL applicant would use a minimum of 0.2 ft-candle (2.152 lux) level required by regulation and that a COL applicant may apply low-light technology as an acceptable alternative for meeting the regulatory requirement. The applicant has identified that the COL applicant would describe the exterior lighting in the site-specific security assessment (i.e., COL information item).

The applicant describes the design basis and assumptions for sizing of electrical loads as described in TR ANP-10295, Section 2.2.1, and includes consideration of a design area to be lit, a specific distance beyond the vehicle barrier system that will be lit, and the efficiency of lamps for the exterior lighting. TR ANP-10295, Figure 2.1, “Scope of Exterior Lighting,” provides configurations and scope for exterior security lighting.

The design basis and assumptions for determining the electrical load for interior lighting are described in TR ANP-10295, Section 2.2.2. The assumptions include the design area to be lit, lighting level for egress, and the efficiency of lamps.

The staff determined and concludes the following:

- The applicant has adequately described the design bases of the security system for meeting 10 CFR 73.55(e)(9)(ii) for protection of all vital area access points and vital area emergency exits with intrusion detection equipment and locking devices that allow rapid egress during an emergency and satisfy the vital area entry control requirements of this section, and the 10 CFR 73.55(e)(9) requirement for control of vital areas, the openings of which must be locked and alarmed.

- As summarized below, the applicant has adequately described the design bases of the applicant’s proposed physical protection systems, components, and features that will be relied on to implement access controls. The applicant design satisfies the requirements of 10 CFR 73.55(g), “Access controls,” as it is applied to the access to the vital island and structures of the U.S. EPR standard design. The proposed design for physical protection includes provisions meeting the access control functions of 10 CFR 73.55(g)(1) at the VA barrier to control personnel by locating access control portals outside of the physical barrier system through which it controls access, equips openings with delay barriers with

locking devices and/or intrusion detection equipment, and includes surveillance equipment and features to prevent unauthorized access as applicable to the designated vital areas.

- The applicant has adequately described the design bases for intrusion detection and assessment systems for meeting the requirements of 10 CFR 73.55(i)(1). These systems provide the capabilities for intrusion detection and assessment unauthorized access to the vital island and vital structures of the U.S. EPR standard design. In addition to meeting the prescriptive requirements of (10 CFR 73.55(i)(1), the proposed design addresses the critical portion of the physical protection system that is intended to meet the performance requirement of 10 CFR 73.55(b) to protection against the DBT. To protect against the DBT, the design provides for the capability to detect and assess unauthorized persons and initiate and facilitate the security response to interdict adversaries along pathways that would allow for implementing a denial strategy.

- The applicant proposed design for intrusion detection and assessment includes the application of technology that complies with 10 CFR 73.55(i)(2) that an intrusion detection equipment must annunciate and video assessment equipment shall display concurrently, in at least two continuously staffed onsite alarm stations, at least one of which must be protected in accordance with the requirements applicable to the central alarm station.

- The applicant has adequately described, within the scope of the design certification, the design bases for meeting 10 CFR 73.55(i)(3), by providing intrusion detection and assessment systems that are designed to provide visual and audible annunciation of the alarm; ensure that annunciation of an alarm indicates the type and location of the alarm; ensure that alarm devices, to include transmission lines to annunciators, are tamper indicating and self-checking; provide an automatic indication when the alarm system or a component of the alarm system fails, or when the system is operating on the backup power supply; support the initiation of a timely alarm for security responses; and ensure intrusion detection and assessment equipment remains operable from an uninterruptible power supply in the event of the loss of normal power.

- The applicant has adequately described physical protection systems to facilitate the implementation of requirements of 10 CFR 73.55(i)(5) for surveillance, observation, and monitoring and has adequately described the design bases for control of unattended openings in accordance with 10 CFR 73.55(i)(5)(iii) that requires unattended openings must be protected by a physical barrier and monitored by intrusion detection equipment or observed by physical protection system personnel at a frequency sufficient to detect exploitation.

- The applicant proposed design and configuration of the CAS and SAS satisfies the requirement of 10 CFR 73.55(i)(4) that both alarm stations must be designed and equipped to ensure that a single act cannot disable both alarm stations. The applicant has adequately addressed by design the regulatory requirement for the survivability of at least one alarm station to maintain the ability to perform the functions of detection, assessment, and capabilities to initiate and coordinate alarm response, request offsite assistance, and provide command and control.

- The applicant's standard design for the location of the CAS meets the requirements of 10 CFR 73.55(4)(ii) that it is within a protected area; the interior of the central alarm station must not be visible from the perimeter of the protected area; it has the capability to allow for assessing and initiating responses to all alarms; it provides assurance that an alarm station operator cannot change the status of a detection point or deactivate a locking or access control device at a protected or vital area portal, without the knowledge and concurrence of the alarm station operator in the other alarm station; and it provides inter-connect of both alarm stations for knowledge of final disposition of all alarms.

- The applicant has adequately described design bases of the CAS and SAS that meet requirements of 10 CFR 73.55(i), "Detection and Assessment Systems," that the construction, location, protection, and equipment of both the central and secondary alarm stations be equal and redundant, such that all security functions needed to satisfy the requirements of 10 CFR 73.55(i) can be performed in both alarm stations.

- The applicant has adequately described the design bases for meeting 10 CFR 73.55(i)(6), "Illumination," that requires all areas of the facility are provided with illumination necessary to satisfy the design requirements of 10 CFR 73.55(b), "General Performance Objectives and Requirements," and implement the protective strategy. The minimum design lighting density has been identified in accordance with 10 CFR 73.55(i)(6)(ii) at an illumination level of 0.2 ft-candles (2.15 lux) in the isolation zones, and appropriate exterior areas within the protected area will be met by the applicant's design. The applicant has indicated that an alternative facility illumination system by means of low-light technology may be applied by a COL applicant to meet the requirements of section 10 CFR 73.55(i)(6) or otherwise implement the protective strategy. The applicant has also described the design bases for interior lighting for physical protection within the vital island and structures for assessment.

- The applicant has adequately described the design bases of the physical protection system for meeting communication requirements in 10 CFR 73.55(j), "Communications requirements." The design of the communications addresses capabilities for establishing and maintaining continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations, capabilities for all on-duty physical protection system force personnel to maintain continuous communication with an individual in each alarm station, and continuous communication capabilities to terminate in both alarm stations. The applicant also adequately addresses prescriptive requirements for providing radio or microwave transmitted two-way voice communication, either directly or through an intermediary, in addition to conventional telephone service between local law enforcement authorities and the site, and a system for communication with the control room. Non-portable communications equipment must remain operable from independent power sources in the event of the loss of normal power.

- The applicant has adequately described the design bases for the secondary power supply, including the uninterruptable power supply source, consistent with

the requirements of 10 CFR 73.55(e)(9)(vi)(A) for the continuity of physical protection systems to perform their intended functions for detection, assessment, communications, and delay (i.e., engineered active delay systems). The design provides for a secondary power supply capable of providing power for 24 hours at the specified design load of physical protection system. This is sufficient and reasonable for continued operations of physical protection systems to facilitate the security responses required to assess and interdiction to meet the performance requirements of 10 CFR 73.55(b).

- In addition, the applicant has adequately described the design bases for the plant lighting power requirements. The design provides for a lighting level which exceeds the minimum of 0.2 ft-candle (2.15 lux) specified by 10 CFR 73.55(i)(6)(ii) for detection and assessment of unauthorized activities, surveillance of plant areas, and security response for interdiction (e.g., acquiring and neutralizing, adversaries).

13.6.4.2.7 Design for Delay Barriers

In TR ANP-10295, the applicant stated the following for the design of delay barriers:

Bullet and Blast Resistant Structures and Systems

The applicant referenced Table 6-5 of "Structure Design for Physical Security," by the American Society of Civil Engineers (ASCE) to determining comparable ballistic properties for construction material, Sandia Laboratories Report SAND 77-0777, "Barrier Technology Handbook," Unified Facilities Criteria (UFC) UFC-40022-01, "Security Engineering: Entry Control Facilities/Access Control Points," Table [as described in TR ANP-10295], "Thickness of Common Materials for Resistance Against UL 752 Level [as described in TR ANP-10295]." In TR ANP-10295, Section 3.0, "Bullet Resistant Walls, Floors, and Ceilings," the applicant compared information and ballistic resistance characteristics provided in the references identified to determine minimum thickness and building construction that would provide bullet resistance to a UL 752, "The Standard of Safety for Bullet-Resisting Equipment," standard as described in TR ANP-10295. Based on review of referenced Table 6-5, the applicant, credits the construction of the building structures (i.e., walls, floors, and ceiling) to meet that minimum thicknesses of concrete, reinforced concrete, and mild steel construction as stated in TR ANP-10295, Section 3.0, for providing capabilities of bullet resistance that are equivalent to UL 752 Level [as specific rounds as described in TR ANP-10295].

In TR ANP-10295, Section 4.0, the applicant identified specific vital island and vital structures that are provided for blast protection. The applicant stated that it assumes a quantity greater than the DBT maximum quantity of explosive for determining the design for safe standoff distances for the location of the VBS from the identified vital structures for blast protection. TR ANP-10295, Section 4.6, provides the resulting minimum safe stand off distances for each of the structures for blast protection.

The applicant's blast protection assessment includes the application of Computer Code A.T. Blast and selective cross-checking according to methodology recommended in TM 5-1300, "Structures to Resist the Effects of Accident Explosions," and NUREG/CR-6190, "Protection Against Malevolent Use of Vehicles at Nuclear Power Plants," December 1994. The assessment of structural design variables consist of sections material, thickness, and reinforcement ratio, structure/element geometry and location, DBT charge weight in equivalent

pounds of trinitrotoluene (TNT), stand-off distance, and blast wave pressures (reflected and incidental), angles, impulse, and durations. The resulting blast protection, safe standoff distances for structures, were determined based on DBT explosives greater than the maximum quantity of DBT explosives. The specific distances for various vital structures are described in TR ANP-10295, Section 4.1, 4.1.1, and Figure 4.1, "Minimum Standoff Distances."

The applicant concluded that the minimum safe standoff distance for the U.S. EPR standard design is based on a quantity greater than the DBT maximum quantity of explosive and located the VBS at the specific distances indicated in TR ANP-10295, Section 4.6.

The applicant stated that the SBODG Building resistance to the DBT explosion is outside the scope of the U.S. EPR standard design certification, and the COL applicant is required to provide a structure that is designed to address the capability to withstand a DBT explosion at the VBS.

The applicant stated that the standoff distances, as analyzed and described in TR ANP-10295, Section 4.6, are sufficient to prevent vehicle bomb blast effects (e.g., air-blast leaking into the structure through failed external doors or openings) and would not cause damage to the safety-related SSCs or loss of spent fuel pool cooling. According to the applicant, the blast protection provided by the structure prevents direct personnel injury from debris and direct effects from the blast waves. The applicant stated that the standoff distances to the opening into the structures exceeds the minimum safe standoff distance for protection of light equipment from the DBT quantity of explosive charge in accordance with NUREG/CR-6190.

Main Control Room, Central and Secondary Alarm Stations Barriers

The applicant indicated that the main control room, central and secondary alarm stations' walls, floors, ceilings, doors, and windows are designed and constructed to meet a minimum bullet resistance to a UL Level as shown on Figure 3.1, "Main Control Room," Figure 3.2, "Central Alarm Station," and Figure 3-3, "Secondary Alarm Station" in TR ANP-10295, Section 3.1.

The applicant stated that the "openings, such as HVAC, will include a labyrinth design such that no linear path exists into the main control room, central and secondary alarm stations without intersecting" either a bullet resistant barrier or a concrete structure of thickness and material construction indicated in TR ANP-10295. The design of the CAS and SAS also credits the walls, floors, and ceilings to provide bullet resistant capabilities to the performance as indicated in TR ANP-10295, Section 3.0.

The applicant indicates the following in TR ANP-10295, Section 3.1:

- Walls, floors, and ceilings of the MCR have a minimum thickness of reinforced concrete that is credited to meet the physical protection requirement for a bullet resistant barrier.

- Walls, floors, and ceilings of the CAS have a minimum thickness of reinforced concrete; and the walls, floors, and ceilings of the SAS have an adequate thickness of reinforced concrete.

- In FSAR Tier 2, Appendix 3B, "Dimensional Arrangement Drawings," the applicant describes the structure design for walls, floors, and ceilings that consist of varying thicknesses in reinforced concrete in FSAR Tier 2, Figures 3.B-20,

3.B-21, 3.B-29, 3.B-47, 3.B-48, and 3.B-51. TR ANP-10295, Section 3.0, Figure 3-1, "Main Control Room," Figure 3-2, "Central Alarm Station," and Figure 3-3, "Secondary Alarm Station," provide plan-views for the specific standard design of the structures, walls, and locations of doors that will meet bullet resistant requirements.

Vehicle Barrier System

The U.S. EPR standard design, in TR ANP-10295, Section 4.0, includes design bases for a VBS to provide protection of structures, including protection against the loss of safety-related equipment necessary to prevent core damage and the loss of spent fuel pool cooling. The applicant indicated that the CAS, SAS, MCR, remote shutdown station, and target sets, as described in TR ANP-10295, Appendix F, are protected against loss of functions by DBT vehicle (land and waterborne) explosives. The applicant stated that a COL applicant will submit a security assessment that addresses the design of passive and active vehicle barrier systems.

Exterior Equipment Doors

In evaluating blast effects on the external equipment doors, the applicant stated that an incidental pressure was calculated using A.T. Blast. Incidental pressure was used because the adjacent aircraft shield and adjacent structures are credited for protection against direct blast pressure and a stand off distance, as described in TR ANP-10295, Section 4.5, based on FSAR Tier 2, Figure 3B-1, "Dimensional Arrangement Reference Plant Building Location," dimensions with the standoff distances indicated in TR ANP-10295, Section 4.6 applied for the limiting structures.

The exterior doors are of substantial metal and concrete construction capable of withstanding the analyzed pressure. The construction of the exterior door, in combination with the aircraft shield provided for opening, provides delay from physical or explosive breaching by adversaries at least equivalent to the vital area entry points.

The exterior walls of the U.S. EPR Nuclear Island are robust as a consequence of the protection provided for aircraft crash. These walls exceed the exterior wall thickness sufficient for protection against the NRC DBT vehicle bomb. Therefore, the exterior door and hatch pressure protections are not directly relatable to the wall thicknesses. Exterior door blast protection is related only to the incident blast pressures from the NRC DBT vehicle bomb at the minimum standoff distances.

Exterior Doors

The U.S. EPR standard design includes hardened exterior doors, interior lockdown doors, hardened equipment hatches, mall gates, deployable turbine grating, and other delay features. TR ANP-10295, Appendix E, shows the specific locations of the delay features. The applicant indicates the following:

- Vital area entry doors are hardened by design to provide delay because time and explosives are needed to breach the door. The specific design basis for delay is stated in TR ANP-10295, Section 7.0. The walls, floors, and roof for the vital areas are reinforced concrete structures of a minimum thickness, as described in TR ANP-10295, and protected opening, with delay characteristics equivalent to delays of the exterior doors.

- Nuclear Island exterior ground level walls are greater than one meter thick of reinforced concrete that delay access and offer performance similar to that analyzed for spent fuel pools. These walls are assumed to be difficult to breach without sophisticated and manual methods and are assumed to be challenging to the adversarial characteristics of the DBT (e.g., explosive quantity needed). The applicant states that the breaching time analysis does not consider the effect of neutralization of adversaries during the extended exposure to defensive fire during the extended breaching time. The details and assumptions of the evaluation are described in TR ANP-10295, Appendix H, "Breaching of Exterior Walls."

- "Equipment hatches are layered hardened structures that aid in preventing access from the exterior by providing delay time to breach the door." The specific delay is described in TR ANP-10295, Section 7.0. The COL information item requires a COL applicant to submit a security assessment that addresses the delay barriers within the protected area presuming hatches are exposed to external reflective blast pressures from the DBT vehicle bomb assuming a standoff distance, as indicated, which is based on FSAR Tier 2, Figure 3B-1 physical dimensions with the standoffs from TR ANP-10295, Section 4.6 applied for the vital structures. The combination of the equipment hatches and the associated aircraft crash shield is capable of withstanding the anticipated reflective pressure without failure.

- Engineered barriers provide both a delay feature and a protective feature as they prevent the challenge to defenders from thrown explosives or incendiary devices. The engineered barriers may be remotely and/or manually operated as described in TR ANP-10295, Section 7.0, depending on the implementation of the interior defensive strategy. The design basis assumes the access delay performance is as stated in TR ANP-10295, Section 7.

- Other engineered barriers provide protection from thrown devices and less for the delay of person. Adversary access delays and deployment of engineered barriers are as stated in TR ANP-10295, Section 7.

- Interior lockdown doors are equipped with access control designed to provide additional delay. The doors are locked. Adversary access delays are protected as indicated in TR ANP-10295, Section 7.

The staff determined and concludes the following:

- The applicant has adequate assessed and documented blast protection for safe standoff distances for the U.S. EPR vital island and structures based on a quantity of explosives greater than the maximum associated with the adversarial characteristics of DBT. The specific distances for vital structures are described in TR ANP 10295, Section 4.1, 4.1.1, and Figure 4.1, "Minimum Standoff Distances," and the acceptable location of a continuous vehicle barrier system that exceeds minimum distances is indicated in TR ANP 10295, Section 4. The applicant has identified that the SBODG Building resistance to the DBT explosion is outside the scope of the U.S. EPR standard design certification, and the COL applicant is required to provide a structure that is designed to address the

capability to withstand a DBT explosion at the VBS. The staff concludes that the applicant has adequate identified required safe standoff distances that are sufficient to prevent vehicle bomb blast effects (e.g., air-blast leaking into the structure through failed external doors or openings) that would cause damage to the safety-related SSCs or loss of spent fuel pool cooling, to facilitate the installation of a VBS at a location that meets the requirement of 10 CFR 73.55(b) to protect against the vehicle explosive threats.

- The applicant has adequately described the design bases for the physical barriers of the vital island and vital structures that are within the scope of the U.S. EPR standard design. The applicant has met, in part, 10 CFR 73.55(e), "Physical Barriers," that requires that each licensee shall identify site-specific conditions to determine the specific use, type, function, and placement of physical barriers. The design bases provide the physical delay of adversaries (i.e., increase travel and/or task times) to allow security responders to deploy, if not pre-deployed, and interdict the adversaries along paths of travel from the PA to the VA and from the VA into the interior of vital island and vital structures, to satisfy the physical protection program design requirements of 10 CFR 73.55(b). A COL applicant referencing the U.S. EPR design will identify site-specific conditions and describe the design of any necessary site-specific physical barriers.

- The applicant has adequately described the design bases of physical barriers to control access to the vital island and vital areas within the scope of the design certification and satisfied the requirement of 10 CFR 73.55(e)(1) by providing the designs of physical barriers necessary to control and delay unauthorized access to satisfy the physical protection program design requirements of paragraph 10 CFR 73.55(b). Specifically, the design bases as described in TR ANP-10295 provide for the control and delay of access necessary to facilitate the implementation of security responses for meeting performance requirements to 10 CFR 73.55(b) to protect against the DBT.

- The applicant description of the design bases for physical barriers, as detailed in TR ANP-10295 adequately addresses the requirements of 10 CFR 73.55(e)(4) by providing the design of physical barrier systems that secure openings or penetrations in to the structural boundaries of the of the vital island and structures. The monitoring to prevent exploitation of the opening is addressed in design of detection and assessment previously described.

- The applicant has adequately described the design bases of the Main Control Room ((MCR) or Reactor Control Room), CAS, and SAS for meeting the requirements of 10 CFR 73.55(e)(5), "Bullet Resisting Physical Barriers." The design bases provide for protecting the MCR, CAS and SAS with a bullet-resistant enclosure by crediting structural elements of the U.S. EPR standard design and providing provisions of hardened doors and engineered system for protecting openings and penetrations of the bullet-resistant enclosure. The design of the last access control to the protected area is outside the scope of the design certification and is to be addressed as COL information item.

- The applicant has adequately described the design bases for physical barriers of the vital island and structures that have been designated as vital areas to address one of two barriers in accordance with requirement of 10 CFR 73.55(e)(9)(i), which requires that the access to vital equipment requires passages through at least two physical barriers.

- The staff determined that 10 CFR 73.2 prescriptive requirements for physical barriers related to site-specific design for fence construction are not applicable to physical barrier systems described for the vital island and vital areas that are within the scope of the design certification. The requirements for site-specific barriers must be addressed and satisfied by a COL applicant.

- The applicant has adequately met the prescriptive requirements in the 10 CFR 73.2, definition for "Physical Barrier," by providing design of physical protection systems and/or credit of building structural systems that satisfy the requirements for building walls, ceilings, and floors to be constructed of brick, cinder block, concrete, steel, or comparable material (openings in which are secured by grates, doors, or covers of construction and fastening with sufficient strength such that the integrity of the wall is not lessened by any opening). The design of physical barriers for the protection of the vital island and structures provides access delays to facilitate the implementation of security responses for meeting performance requirements to 10 CFR 73.55(b) to protect against the DBT.

13.6.4.3 *Design Features to Facilitate Security Response*

The applicant indicates the following for the design of physical protection systems for enhancing or facilitating the response of security responders that is within the scope of the design certification:

- Internal defensive positions consist of a combination of deployable and fixed ballistic barriers at positions indicated in TR ANP-10295, Appendix D, for the U.S. EPR standard design. The barriers are designed to be bullet resistant to a UL 752 level as described in Appendix D. The design also includes engineered delay barriers and features to protect against hand thrown explosive or incendiary devices as indicated in figures in TR ANP-10295, Appendix E. The design of internal defensive positions include deployable barriers, protection from fragments, and a specific height for protection of security responders. The designed locations or placements of delay features provide standoff from explosive deployable barrier to increase survivability of security responders. Fixed defensive positions design include additional protection against hand thrown explosive devices. The locations of defensive positions within the vital island and vital structures that are within the scope of the design certification are provided in TR ANP-10295, Appendix D.

- TR ANP-10295, Section 6.0, also describes the design of external BRE defensive positions that are equipped with HVAC systems to allow isolation capability to minimize the exposure of security responders to external environmental threats to the extent possible. The applicant evaluation of external protective strategy, defensive analyses, "includes an analysis with the most

effective staffed defensive post excluded. This bounds the security staff performance by analyzing a single equipment failure, low probability neutralization by adversaries (e.g., "lucky shot"), as well as the passive insider being located at the most effective post." The design bases for the engineered defensive positions and their locations are described for the U.S. EPR standard design in TR ANP-10295, Section 6.0. The design of BRE defensive positions, providing protection of the exterior of the vital island and structures and their locations are not within the scope of the design certification, and will be addressed by the COL applicant's security assessment as specified in COL Information Item 13.6-1.

The staff determined and concludes the following:

- The staff determined that the applicant has described the design bases for deployable defensive positions and protection barriers that will be relied on to facilitate the implementation of security responses to interdict adversaries within the vital island and vital structures.

- The applicant has established COL Information Item No. 13.6-1 that identifies that the COL applicant provides the design bases for engineered controls for the final design, construction, and installation of BRE defensive positions for protection of security responders that will interdict adversaries outside of the vial island and structures (i.e., at the PA boundaries and plant areas between the PA and VA barriers).

13.6.4.4 *Combined License Information Items*

The staff reviewed the applicant's descriptions and commitments for COL information items that must be addressed by a COL applicant if the design is certified. The applicant provided the following three COL information items in FSAR Tier 2, Table 1.8-2 and TR ANP-10295:

- COL Information Item No. 13.6-1: "A COL applicant that references the U.S. EPR design certification will provide a site-specific security assessment that adequately demonstrates how the performance requirements of 10 CFR 73.55(a) are met for the initial implementation of the security program."

- COL Information Item No. 13.6-2: "A COL applicant that references the U.S. EPR design certification will provide a security plan to the NRC to fulfill the requirements of 10 CFR 52.79(a)(35)."

- COL Information Item No. 13.6-3: "A COL applicant that references the U.S. EPR design certification will provide a security program, through the [physical security plan] PSP and supporting documents such as the vital equipment list and the vital areas list that incorporates the security features listed in the U.S. EPR FSAR Tier 2, Section 13.6."

- COL Information Item No. 13.6-4: "A COL applicant that references the U.S. EPR design certification will provide a cyber security plan consistent with 10 CFR 73.54."

In FSAR Tier 2, Table 1.8-2, the applicant indicates that the COL applicant that references the U.S. EPR design certification will meet COL Information Item No. 13.6-3 by providing a security program, and incorporates the security features described in FSAR Tier 2, Section 13.6. COL Information Item No. 13.6-4 is only identified in TR ANP-10295, but not identified in FSAR Tier 2, Table 1.8-2. The COL Information Item No. 13.6-1 will require the COL applicant to address a site-specific security assessment that compliments the design of systems described in TR ANP-10295 and provides appropriately the design basis and addresses the 10 CFR Part 73 performance requirements for the following:

- PA personnel and vehicle access control systems, PA delay barriers, PA perimeter intrusion detection, and PA isolation
- Station blackout diesel generator, location, and structures
- Exterior lighting
- Standard defense scenarios, defensive configuration, placement, and visual coverage, and required staffing of external defensive positions
- Internal and external surveillance camera placement
- Target sets, by reference to the TR ANP-10295 or modified with additional site-specific information
- Security system acceptance testing

The staff determined and concludes that the applicant has adequately identified and described COL information items in order to complete the design of the remaining parts of a physical protection system, including a physical protection program, that are not within the scope of the design certification. The applicant has adequately justified and determined appropriate demarcation of actions required of a COL applicant and has identified COL information items in appropriate chapters of the FSAR (FSAR Tier 2 documentation) and referenced TR ANP-10295.

13.6.5 Combined License Information Items

Table 13.6-1 provides a list of security-related COL information item numbers and descriptions from FSAR Tier 2, Table 1.8-2:

Table 13.6-1 U.S. EPR Combined License Information Items

Item No.	Description	FSAR Tier 2 Section
13.6-1	A COL applicant that references the U.S. EPR design certification will provide a site-specific security assessment that adequately demonstrates how the performance requirements of 10 CFR 73.55(a) are met for the initial implementation of the security program.	13.6

Item No.	Description	FSAR Tier 2 Section
13.6-2	A COL applicant that references the U.S. EPR design certification will provide a security plan to the NRC to fulfill the requirements of 10 CFR 52.79(a)(35).	13.6
13.6-3	A COL applicant that references the U.S. EPR design certification will provide a security program through the PSP and supporting documents such as the vital equipment list and the vital area list, that incorporate the security features specified in the FSAR Tier 2, Section 13.6.	13.6
13.6-4	A COL applicant that references the U.S. EPR design certification will provide a cyber security plan consistent with 10 CFR 73.54 (Confirmatory Item 14.03.05-3).	13.6

The staff finds the above list of COL information items to be complete. Also, the list adequately describes the actions necessary for the COL applicant or holder.

13.6.6 Conclusions

As described above, and with the exception of the identified open items, the staff concludes that the applicant has considered and provided physical protection systems or features in the standard U.S. EPR design, within the scope of the design certification, to facilitate the implementation of a physical protection program to protect against potential acts of radiological sabotage. The U.S. EPR proposed standard design has adequately described the plant layout for enhancing physical protection and identified vital equipment and areas for meeting, in part, specified requirements of 10 CFR 73.55. The technical bases, including assumptions, are adequately described and provide support of ITAAC for physical protection systems and hardware.

With the exception of the open items, the applicant's proposed design of physical protection systems, including locations and configurations, is adequate to address the vital island and vital structures within the scope of the design certification with adequate details of technical or design basis to allow for detailed design and inspection verification of construction and installation (ITAAC verification) in accordance with requirements of 10 CFR Part 52. This conclusion is limited to the adequacy of applicant descriptions of the design basis of the physical protection systems and components that are relied on to implement security response functions (i.e., detection, assessment, communications, delays, and neutralization) within the scope of the design certification. The demonstration of a high assurance of adequate protection against the DBT and compliance with programmatic requirements (including administrative controls such as people and procedures) of the NRC regulation for physical protection are to be addressed by a COL applicant that is seeking a combined license to construct and operate a nuclear power plant.

Except for RAI 425, Questions 13.06.02-1, 13.06.02-2, and 13.06.02-4 identified above, the staff concludes that the U.S. EPR physical protection systems design is acceptable in accordance with the applicable requirements of 10 CFR Part 73 within the scope of the U.S. EPR design certification. **RAI 425, Questions 13.06.02-1, 13.06.02-2, and 13.06.02-4 are being tracked as open items**.

13.7 Fitness for Duty

10 CFR Part 26, "Fitness for Duty Programs," prescribes requirements and standards for the establishment, implementation, and maintenance of fitness-for-duty (FFD) programs (reference 73 *FR* 17176, March 31, 2008). 10 CFR 26.3 states, in part, that holders of a COL under 10 CFR Part 52 shall implement the FFD program before the receipt of special nuclear material in the form of fuel assemblies. Whether the COL holder is constructing the plant, has received special nuclear material onsite, or is operating the plant will determine the FFD requirements that it must implement. In addition, an applicant for a COL who has been issued a limited work authorization (LWA) under 10 CFR 50.10(e) must implement an FFD program if the LWA authorizes the applicant to install the foundations for safety- and security-related SSCs.

Pursuant to 10 CFR 52.79(a)(44), COL applications must contain "[a] description of the fitness-for-duty program required by 10 CFR Part 26 and its implementation."

The FSAR for the U.S. EPR design certification contains COL information items, which AREVA has deferred to the COL applicant to address in its application. The staff agrees that the FFD program is the COL applicant's responsibility. Table 13.7-1 provides a list of fitness for duty related COL information item numbers and descriptions from FSAR Tier 2, Table 1.8-2:

Table 13.7-1 U.S. EPR Combined License Information Items

Item No.	Description	FSAR Tier 2 Section
13.7-1	A COL applicant that references the U.S. EPR design certification will submit a physical security plan to the NRC to fulfill the fitness for duty requirements of 10 CFR Part 26.	13.7

The staff determines the above listing to be complete. Also, the list adequately describes actions necessary for the COL applicant or holder. No additional COL information items need to be included in FSAR Tier 2, Table 1.8-2 for fitness for duty consideration.