13.8 Cyber Security

13.8.1 Introduction

Section 13.8, "Cyber Security," of this safety evaluation report (SER) includes evaluations associated with the Cyber Security Program which is implemented prior to receipt of fuel on site.

Luminant Generation Company, LLC's (hereinafter referred to as the applicant) submitted the Comanche Peak Nuclear Power Plant (CPNPP), Units 3 and 4, Combined License (COL) Application (COLA), Revision 3, Part 9, 'Withheld Information,' 'Comanche Peak Nuclear Power Plant, Units 3 and 4 Cyber Security Plan (CSP),' to the U.S. Nuclear Regulatory Commission (NRC or Commission). The purpose of the CSP is to provide high assurance that the digital computer and communication systems and networks associated with safety, security, and emergency preparedness (SSEP) functions, as well as support systems and equipment, which if compromised, would adversely impact safety, security, or emergency preparedness functions are adequately protected against cyber attacks.

The scope of the review is programmatic. For the purposes of a COL Final Safety Analysis Report (FSAR) review, the staff does not review design information contained in the CSP.

13.8.2 Summary of Application

In Part 9 of the COLA, Revision 3, the applicant submitted a CSP. Furthermore, in CPNPP, Units 3 and 4, COL Part 2 FSAR, Revision 3, Section 13.4.1 "Combined License Information," Table 13.4-201, "Operational Programs Required by NRC Regulation and Program Implementation," Item 15, 'Security Program,' the applicant provided the following license condition:

> Prior to the receipt of fuel on-site in the protected area, the Cyber Security Program will be implemented to meet the requirements of 10 CFR 73.54.

US-APWR COL Information Item

- Standard (STD) COL 13.6(1)

Section 13.6, "Security," of the CPNPP, Units 3 and 4, COL FSAR, Revision 3, states:

> Replace the first paragraph in DCD Subsection 13.6 with the following:
>
> The comprehensive physical security program is addressed in the Security Plan. The Security Plan consists of the physical security plan, training and qualification plan, and the safeguards contingency plan. The Security Plan (provided in Combined License Application Part 8) and Cyber Security Plan are submitted to the NRC to fulfill the requirements of 10 CFR 52.79(a)(35) and 10 CFR 52.79(a)(36). The Security Plan and Cyber Security Plan meet the requirements contained in 10 CFR 26 and 10 CFR 73 and will be maintained in accordance with the requirements of 10 CFR 52.98. The Security Plan is categorized as security safeguards information and is withheld from public disclosure pursuant to 10 CFR 73.21.

The applicant provided additional information in STD COL 13.6(1) to address COL Information Item 13.6(1), which states:

> The COL Applicant is to develop and provide the plant overall security plan (consisting of the physical security plan, safeguards contingency plan, and the guard training and qualification plan) and the cyber security plan and the implementation schedule for security programs.

13.8.3 Regulatory Basis

The relevant requirements of the Commission's regulations for physical security, and the associated acceptance criteria, are given in Section 13.6.1, “Physical Security – Combined License and Operating Reactors,” of NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants.” The acceptance criteria for the regulatory review are given in Section 13.6.6, “Cyber Security Plan,” of NUREG-0800.

Acceptance criteria are based on meeting the relevant requirements of the following Commission regulations:

1. Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54, “Protection of digital computer and communication systems and networks,” which requires an applicant to provide a high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat described in 10 CFR Part 73.1.

2. 10 CFR 73.55(a)(1), which requires an applicant to submit a CSP and establish, maintain, and implement a CSP.

3. 10 CFR 73.55(b)(8), which requires an applicant to submit a CSP and establish, maintain, and implement a CSP.

4. 10 CFR 73.55(m), “Security program reviews,” which requires the licensee to review each element of the physical protection program at least every 24 months.

5. Appendix G, “Reportable Safeguards Events,” to 10 CFR Part 73, “Physical Protection of Plants and Materials,” which discusses the reporting requirements following safeguard events.

6. 10 CFR 73.58, “Safety/Security Interface Requirements for Nuclear Power Reactors,” which requires licensees to assess and manage the potential adverse effects on safety and security before implementing changes to the plant configurations, facility conditions, or security.

7. Regulatory Guide (RG) 5.71, ‘Cyber Security Programs for Nuclear Facilities,’ January 2010, which provides guidance to applicants and licensee on satisfying the requirements of 10 CFR 73.54.

The security plan is considered acceptable if it conforms to RG 5.71, “Cyber Security Programs for Nuclear Facilities.”

13.8.4 Technical Evaluation

The NRC staff reviewed the information in CPNPP, Units 3 and 4, COLA Part 2 FSAR Section 13.6 and Part 9 CSP against the detailed guidance described in RG 5.71. The applicant's CSP substantially conforms to the NRC template in RG 5.71, Appendix A, "Generic Cyber Security Plan Template," which provides an acceptable method for complying with the NRC's regulations. The following subsections describe the key aspects of the CSP that conform to the NRC guidance, and where the CSP deviates from the template, that particular deviation is evaluated for compliance with the regulatory requirements.

13.8.4.1 Cyber Security Plan Scope and Purpose

By letter dated December 14, 2009, as supplemented by letter dated July 28, 2010, and COLA, Revision 3, Part 9 the applicant submitted it's CSP for CPNPP, Units 3 and 4. This CSP describes how the applicant, established a cyber security program to achieve high assurance that CPNPP, Units 3 and 4, digital computer and communication systems and networks associated with SSEP functions (hereafter defined as critical digital assets (CDAs)) are adequately protected against cyber attacks up to and including the design basis threat (DBT).

On October 21, 2010, the NRC issued Staff Requirements Memorandum (SRM), CMWCO-10-0001, "Regulation of Cyber Security at Nuclear Power Plants." This SRM stated that the Commission determined that NRC's cyber security rule in 10 CFR 73.54 should be interpreted to include structures, systems, and components in the balance of plant (BOP) that have a nexus to radiological health and safety at NRC licensed nuclear power plants. Because the applicant's CSP did not include the information described in the Commission's SRM, the staff issued request for additional information **(RAI) 6013-227**. In its response to **RAI 6013-227**, dated September 16, 2011, the applicant revised its CSP, Section A.1 'Introduction,' to include the following paragraph:

> Within the scope of the NRC's cyber security rule at 10 CFR 73.54, systems or equipment that perform important to safety functions include structures, systems, and components (SSCs) in the balance of plant (BOP) that could directly or indirectly affect reactivity at a nuclear power plant and could result in an unplanned reactor shutdown or transient. Additionally, these SSCs are under the licensee's control and include electrical distribution equipment out to the first inter-tie with the offsite distribution system.

In order to comply with the SRM, the applicant, in its CSP, deviated from RG 5.71 to clarify that systems or equipment that perform important to safety functions, include SSCs in the BOP that could directly or indirectly affect reactivity and could result in an unplanned reactor shutdown or transient. As explained below, this deviation from RG 5.71 is consistent with the Commission's policy.

The following actions, described in the CSP, Section A.2, 'Cyber Security Plan,' provide high assurance of adequate protection of systems associated with the above functions from cyber attacks:

- Implementing and documenting the "baseline" security controls described in Regulatory Position C.3.3 of RG 5.71, and

- implementing and documenting a cyber security program to maintain the established cyber security controls through a comprehensive life cycle approach, as described in Section 4 of [the CSP].

The staff reviewed the CPNPP, Units 3 and 4, CSP against the template in RG 5.71 and the SRM, CMWCO-10-0001, "Regulation of Cyber Security at Nuclear Power Plants," dated October 21, 2010. On the basis of its review of this section, the staff finds that the CPNPP, Units 3 and 4, CSP appropriately follows the guidance in RG 5.71 and Commission Policy and is acceptable. Accordingly**, RAI 6013-227 is resolved and closed.**

13.8.4.2 Performance-Based Requirements

The CPNPP, Units 3 and 4, COLA, Revision 3, CSP, Section A.2, states the following:

> As required by 10 CFR 73.55(a)(1), a licensee must implement the requirements of this section through its Commission-approved physical security plan, training and qualification plan, safeguards contingency plan, and cyber security plan, referred to collectively as "security plans." As defined in 10 CFR 73.54(b)(3), cyber security is a component of the physical protection program. As such, this plan establishes how CPNPP Units 3 and 4 digital computer and communication systems and networks within the scope of 10 CFR 73.54 will be adequately protected from cyber attacks up to and including the DBT.

On the basis of its review of this section, the staff finds that the CPNPP, Units 3 and 4, COLA, Revision 3, CSP appropriately follows the guidance for establishing and implementing a cyber security program in RG 5.71 and is, therefore, acceptable.

13.8.4.3 Cyber Security Program Implementation

The applicant committed to implementing its cyber security program by stating the following in COLA, Revision 3, CSP, Section A.3, 'Cyber Security Program Implementation':

> Luminant established and maintains a cyber security program that complies with the requirements of 10 CFR 73.54(b)(2) and 10 CFR 73.55(b)(8) to protect those systems within the scope of 10 CFR 73.54(a)(1)(i-iv) that can, if compromised, directly or indirectly, have an adverse impact on the SSEP functions of a nuclear facility. This cyber security program complies with 10 CFR 73.54 by (1) establishing and implementing defensive strategies consistent with the defensive model described in Section 3.1.5 of this document, including the security controls described in Sections 3.1, 3.2, and 3.3, and (2) maintaining the program, as described in Section 4 of this document [the CSP].
>
> Documentation of the security controls in place for each CDA is available for inspection. Modifications to the cyber security plan are conducted in accordance with 10 CFR 50.54(p). As required by 10 CFR 50.90, "Application for Amendment of License, Construction Permit, or Early Site Permit," Luminant will submit changes that are determined to decrease the effectiveness of this plan to the NRC for approval. Luminant will also report any cyber attacks or incidents at CPNPP Units 3 and 4 to the NRC, as required by 10 CFR 73.71, "Reporting of Safeguards Events," and Appendix G, "Reportable Safeguards Events," to 10 CFR Part 73, "Physical Protection of Plants and Materials."

As stated in COLA Revision 3, Part 2 FSAR Table 13.4-201, Item 15, the applicant proposed to implement the following license condition in the Security Program:

- **License Condition (13-4)** - Prior to receipt of fuel on-site in the protected area, the Cyber Security Program will be implemented to meet the requirements of 10 CFR 73.54.

The applicant provided a license condition that addressed the implementation of the plant-specific cyber security program. This license condition is consistent with SECY-05-0197, "Review of Operational programs in a Combined License Application and Generic Emergency Planning Inspections, Tests, Analyses, and Acceptance Criteria," dated October 28, 2005, which discusses license conditions for operational programs. Since security is an operational program, the staff finds the applicant's proposed license condition to be acceptable.

In addition, the staff intends to implement the following license condition below:

- **License Condition (13-5)** - No later than 12 months after issuance of the COL, the licensee shall submit to the Director of NRO a schedule that supports planning for, and the conducting of, the NRC inspection of the cyber security program implementation. The schedule shall be updated every 6 months until 12 months before scheduled fuel loading, and every month thereafter until the cyber security program has been fully implemented."

As discussed in SECY-05-0197, "Review of Operational Programs in a Combined License Application and Generic Emergency Planning Inspections, Tests, Analyses, and Acceptance Criteria" a COL applicant should provide schedules for implementation milestones for operational programs. SECY 05-0197 further adds that maintaining NRC inspection schedules will be critical to ensuring that the Commission has timely information on operational readiness. As such, the staff intends to impose **License Condition 13-5** to support its plans to inspect operational programs and their implementation to ensure these programs are being implemented consistently with the COLA FSAR Table 13.4-201. The staff, in **RAI 6123-238**, requested that the applicant include this license condition in the next revision of its COLA. Since the staff is imposing this license condition upon the applicant, **RAI 6123-238** is resolved and closed.

On the basis of its review of this section, the staff finds that the CPNPP, Units 3 and 4, COLA, Revision 3, CSP appropriately follows the guidance, for establishing and maintaining a CSP in RG 5.71 and is, therefore, acceptable.

In addition, the applicant has developed and submitted its cyber security plan, and has developed an implementation schedule as shown in COLA Revision 3, Part 2 FSAR Table 13.4-201, Item 15. As such, the applicant has adequately addressed STD COL 13.6(1). The applicant's Security Plan has been evaluated in Section 13.6 of the staff's Chapter 13 safety evaluation.

13.8.4.4 Cyber Security Assessment and Authorization

The CPNPP, Units 3 and 4, COLA, Revision 3, CSP, Section A.3 states:

Luminant developed and annually reviews and updates the following:

- a formal, documented security planning, assessment and authorization policy that describes the purpose, scope, roles, responsibilities, management commitments, and coordination among Luminant site organizations and Corporate and the implementation of this CSP, and the security controls in Appendices B and C to RG 5.71, and

- a formal, documented procedure to facilitate the implementation of the CSP and the security assessment.

On the basis of its review of this section, the staff finds that the CPNPP, Units 3 and 4, COLA, Revision 3, CSP appropriately follows the guidance for security assessment and authorization in RG 5.71 and is, therefore, acceptable.

13.8.4.5 Cyber Security Team

The CPNPP, Units 3 and 4, CSP discusses the cyber security team (CST), which should have the authority to conduct an objective assessment of the program, make determinations about the program, implement D3 protective strategies, and implement the security controls using the process outlined in Regulatory Position C.3.3 of RG 5.71.

The applicant has submitted a CSP for CPNPP, Units 3 and 4, that indicates that the CST consists of individuals with broad knowledge in the following areas:

- Information and digital system technology
    - Cyber security
    - Software development
    - Communications
    - Systems administration
    - Computer engineering
    - Networking-site and corporate networks
    - Programmable logic controllers
    - Control systems
    - Distributed control systems
    - Computer systems and databases used in design, operation, and maintenance of CDAs

- Nuclear facility operations, engineering, and technical specifications

- Physical security and emergency preparedness systems and programs

The CPNPP, Units 3 and 4, CSP lists the roles and responsibilities for the CST, which include the following:

- Perform or oversee each stage of cyber security management processes.

- Document all key observations, analyses, and findings during the assessment process so that information can be used in the application of security controls.
- Evaluate or reevaluate assumptions or conclusions about current cyber security threats.
- Evaluate or reevaluate assumptions or conclusions about potential vulnerabilities to, and consequences from, an attack.
- Evaluate or reevaluate assumptions or conclusions about the effectiveness of existing cyber security controls, defensive strategies, and attack mitigation methods, as well as cyber security awareness and training of those working with, or responsible for, CDAs and cyber security controls throughout their system life cycles.
- Confirm information from reviews of CDAs and connected digital devices and associated security controls with physical and electronic validation activities.
- As needed, identify and implement new cyber security controls.
- Document the implementation of alternate or compensating measures in lieu of any security controls (Appendices B and C of RG 5.71).
- Document the basis for not implementing certain controls (Appendix B of RG 5.71).
- Prepare documentation and oversee implementation of security controls (Appendices B and C of RG 5.71).
- Retain all documentation in accordance with 10 CFR 73.55(q) and Section C.5 of RG 5.71.

The CPNPP, Units 3 and 4, CSP notes that security assessment determinations should not be constrained by operational goals.

On the basis of its review of this section, the staff finds that the CPNPP, Units 3 and 4, COLA Revision 3, CSP appropriately follows the guidance in RG 5.71 by defining and documenting roles, responsibilities, authorities, and functional relationships within the cyber security team. As such, the staff finds this acceptable.

13.8.4.6 Identification of Critical Digital Assets

The CPNPP, Units 3 and 4, COLA, Revision 3, CSP, Section A.3 describes that the applicant will document the identification of critical digital assets as described in Regulatory Position C.3.1.3 of RG 5.71 and includes the following:

- Identify and document systems, equipment, communication systems, and networks that are associated with the SSEP functions described in 10 CFR 73.54(a)(1), as well as the support systems associated with these SSEP functions. Systems, equipment, and networks associated with SSEP functions are referred to as critical systems (CS). The CST identified CSs by conducting an initial consequence analysis of systems, equipment, communication systems, and networks to determine those which, if compromised, exploited, or failed, could impact the SSEP functions of the nuclear facility, without taking into account existing mitigating measures.

- Perform a dependency and pathway analysis of any system or equipment associated with SSEP functions to determine whether they are CS.

- Identify and document CDAs that have a direct, supporting, or indirect role in the proper functioning of CS.

The submitted CSP discusses documenting the following:

- Description of CDA.

- Identification of each CDA within each CS.

- Description of CDA function.

- Identification of the consequences to the CS and SSEP functions, if a compromise were to occur.

- Identification of the digital devices having direct or indirect roles in CS function.

- Description of security functional requirements or specifications that includes the following:

    - Security requirements for vendor or developers to maintain system integrity.
    - Secure configuration, installation, and operation of the CDA.
    - Effective use and maintenance of security features or functions.
    - Known vulnerabilities regarding configuration and use of administrative functions.
    - Effective use of user-accessible security features or functions.
    - Methods for user interaction with CDA.
    - User responsibilities in maintaining the security of the CDA.

On the basis of its review of this section, the staff finds that the CPNPP, Units 3 and 4, COLA, Revision 3, CSP appropriately follows the guidance for identifying critical digital assets in RG 5.71 and is, therefore, acceptable.

13.8.4.7 Reviews and Validation Testing

COLA, Revision 3, CSP, Section A.3 identifies and documents the method to accomplish tabletop reviews and validation testing for each CDA as described in Regulatory Position C.3.1.4 of RG 5.71. For each CDA/CS group, the CST will identify and document:

- A direct/indirect connection pathway.
- Infrastructure interdependencies.
- Application of defensive strategies, including defensive models, security controls, and other defensive measures.

The submitted CSP indicates validation activities are accomplished by performing comprehensive walkdowns, including the following:

- Performing physical inspection of the connections and configuration of each CDA.
- Tracing all communication connections into and out of each CDA to the termination point along all communication pathways for each CDA.
- Examining the physical security of the CDA, including the communication pathways.
- Examining the configuration and assessing the effectiveness of existing security controls along the communication pathways.
- Examining interdependencies for each CDA and trust relationships between CDAs.
- Examining interdependencies with infrastructure support systems emphasizing compromises of electrical power, environmental controls, and fire suppression equipment.
- Examining systems, networks, and communication systems and networks that are potential pathways for attacks.
- Resolving CDA information and configuration discrepancies found in the review, including undocumented or missing connections, and other cyber security-related irregularities associated with the CDA.

The submitted CSP notes that an electronic validation is performed when a physical walkdown inspection is impractical. This electronic validation consists of tracing a communication pathway from start to finish. Use of electronic equipment may prove a better method than a physical walkdown.

On the basis of its review of this section, the staff finds that the CPNPP, Units 3 and 4, COLA, Revision 3, CSP appropriately follows the guidance for review and validation in RG 5.71 and is, therefore, acceptable.

13.8.4.8 Defense in Depth Protective Strategies

COLA, Revision 3, CSP, Section A.3 provides for the implementation of defensive strategies that ensure the capability to detect, respond to, and recover from a cyber attack. The defensive strategies consist of the following:

- Security controls implemented in accordance with Section 3.1 of the CSP and the defensive model outlined in Regulatory Position C.3.2 of RG 5.71.
- D3 measures described in Section C.6, "Defensive Strategy," of Appendix C, "Operational and Management Security Controls," of RG 5.71.
- Detailed defensive architecture described in Section C.7, "Defense-in-Depth," of Appendix C of RG 5.71.
- Maintenance of a cyber security program in accordance with Section 4, 'Maintaining the Cyber Security Program,' of Appendix A, "Generic Cyber Security Plan Template," of RG 5.71.

The submitted CSP notes that the defensive model establishes the logical and physical boundaries between CDAs with similar risks and CDAs with lower security risks.

On the basis of its review of this section, the staff finds that the CPNPP, Units 3 and 4, COLA, Revision 3, CSP appropriately follows the guidance for defense in depth protective strategies in RG 5.71 and is, therefore, acceptable.

13.8.4.9 Application of Security Controls

The applicant established D3 strategies by implementing and documenting the following:

- Defensive model, described in Regulatory Position C.3.2 of RG 5.71.
- Physical security program and physical barriers.
- Security controls implemented in accordance with Section A.3.1, "Analyzing Digital Computer Systems," of the CSP.
- Operational and management controls described in Appendix C of RG 5.71.
- Technical controls described in Appendix B, "Technical Security Controls," of RG 5.71.

The CPNPP, Units 3 and 4, COLA, Revision 3, CSP, Section A.3.1.6, "Application of Security Controls," discusses the use of information collected from Section A.3.1.4, "Reviews and Validation Testing," of the CSP to conduct one or more of the following activities for each CDA:

- Implement all security controls specified in Appendix B of RG 5.71.
- If a security control cannot be applied, implement an alternative control listed in Appendix B of RG5.71 by doing one of the following:

- Document the basis for employing alternate countermeasures.
- Perform and document an attack vector and attack tree analysis of the CDA to confirm that the countermeasure provides the same or greater protection as the corresponding control.
- Implement alternative countermeasures that provide at least the same degree of protection as the corresponding security control in Appendix B of RG 5.71.

- Not implementing controls enumerated in Appendix B of RG 5.71 by performing the following:

  - Performing an attack vector and attack tree analyses of the specific security controls for the CDA that will not be implemented.
  - Documenting that the attack vector does not exist and demonstrating that the control is not necessary.

The submitted CPNPP, Units 3 and 4, COLA, Revision 3, CSP notes that, before implementing security controls on a CDA, the potential for adverse impact must be assessed. Specifically, the applicant should consider the following:

- Do not implement a security control if there is a known adverse impact to SSEP functions.

- Use alternate controls to mitigate the lack of the security control, in accordance with Section A.3.1.6 of the CSP.

The submitted CPNPP, Units 3 and 4, COLA, Revision 3, CSP includes provisions to verify that CDAs are adequately protected from cyber attacks, up to and including the DBT, and that any identified gaps have been closed. The security program will require the following:

- Performing an effectiveness analysis, as described in Section A.4.1.2, “Effectiveness Analysis,” of the CSP.

- Performing a vulnerability assessment or scans, as described in Section A.4.1.3, “Vulnerability Assessments and Scans,” of the CSP.

- Implement alternative countermeasures that provide at least the same degree of protection as the corresponding security control.

On the basis of its review of this section, the staff finds that the CPNPP, Units 3 and 4, COLA, Revision 3, CSP appropriately follows the guidance for application of security controls in RG 5.71 and is, therefore, acceptable.

13.8.4.10 Incorporating the Cyber Security Program into the Physical Protection Program

The CPNPP, Units 3 and 4, COLA, Revision 3, CSP discusses the following efforts necessary to integrate the management of physical and cyber security:

- Consideration of cyber attacks during the identification of target sets.
- Establishment of site organizational responsibilities for cyber security.
- Documentation of physical and cyber security interdependencies.
- Incorporation of policies and procedures to secure the CDAs from attacks up to and including the DBT.
- Coordination of personnel training.
- Integration and coordination of incident response personnel.
- Training of senior management.
- Performance of periodic exercises of simulated physical and cyber attacks.

The CPNPP, Units 3 and 4, COLA, Revision 3, CSP states the cyber security program is reviewed as a component of the physical security program in accordance with the requirements of 10 CFR 73.55(m).

On the basis of its review of this section, the staff finds that the CPNPP, Units 3 and 4, COLA, Revision 3, CSP appropriately follows the guidance incorporating the cyber security program into the physical protection program in RG 5.71 and is, therefore, acceptable.

13.8.4.11 Policies and Implementing Procedures

The COLA, Revision 3, CSP indicates the following:

- Luminant Power developed and implemented policies and procedures to meet the security control objectives provided in Appendices B and C of RG 5.71.
- Luminant Power documented, reviewed, approved, issued, used, and revised policies and implementation procedures as described in Section A.4, “Maintaining the Cyber Security Program,” of the CSP.
- Luminant Power ensured personnel responsible for implementing and overseeing the program report to the site vice president responsible for nuclear plant operation.
- Luminant Power established specific responsibilities for positions described in Section C.10.10, “Roles and Responsibilities,” of Appendix C of RG 5.71.

On the basis of its review of this section, the staff finds that the CPNPP, Units 3 and 4, COLA, Revision 3, CSP appropriately follows the guidance for policies and implementing procedures in RG 5.71 and is, therefore, acceptable.

13.8.4.12 Maintaining the Cyber Security Program

The CPNPP, Units 3 and 4, COLA, Revision 3, CSP states the following:

> This section establishes the programmatic elements necessary to maintain security throughout the life cycle of CDAs. Luminant implemented the elements of this section [of the CSP] to maintain high assurance that CDAs associated with the SSEP functions of CPNPP, Units 3 and 4, are adequately protected from cyber attacks.
>
> Luminant employs a life cycle approach consistent with the controls described in Appendix C to RG 5.71. This approach ensures that the security controls established and implemented for CDAs are adequately maintained to achieve the site's overall cyber security program objectives. For proposed new digital assets, or existing digital assets that are undergoing modification, Luminant implements the process described in Section 4.2 of this plan.
>
> Luminant Power, CPNPP, Units 3 and 4, maintains records in accordance with Section 5 of this plan.

On the basis of its review of this section, the staff finds that the CPNPP, Units 3 and 4, COLA, Revision 3, CSP appropriately follows the guidance for maintaining the cyber security program in RG 5.71 and is, therefore, acceptable.

13.8.4.12.1 Continuous Monitoring and Assessment

The CPNPP, Units 3 and 4, COLA, Revision 3, CSP indicates:

> Luminant continuously monitors security controls consistent with Appendix C to RG 5.71. Automated support tools are also used, as appropriate, to accomplish near real-time cyber security management for CDAs. The continuous monitoring program includes the following:
>
> - ongoing assessments to verify that the security controls implemented for each CDA remain in place throughout the life cycle,
> - verification that rogue assets have not been connected to the infrastructure,
> - periodic assessments of the need for and effectiveness of the security controls identified in Appendices B and C to RG 5.71, and
> - periodic security program review to evaluate and improve the effectiveness of the program.
>
> This element of the program is mutually supportive of the activities conducted to manage configuration changes of CDAs. Continuous monitoring may require periodic updates to the cyber security plan.

On the basis of its review of this section, the staff finds that the CPNPP, Units 3 and 4, COLA, Revision 3, CSP appropriately follows the guidance for continuous monitoring and assessment in RG 5.71 and is, therefore, acceptable.

13.8.4.12.2 Periodic Assessment of Security Controls

The CPNPP, Units 3 and 4, COLA, Revision 3, CSP states:

> Luminant performs periodic assessments to verify that the security controls implemented for each CDA remain robust, resilient, and effective in place throughout the life cycle. The CST verifies the status of these security controls on at least an annual basis or in accordance with the specific requirements for each security control, as described in Appendices B and C to RG 5.71, whichever is more frequent.

On the basis of its review of this section, the staff finds that the CPNPP, Units 3 and 4, COLA, Revision 3, CSP appropriately follows the guidance for periodic assessment of security controls in RG 5.71 and is, therefore, acceptable.

13.8.4.12.3 Effectiveness Analysis

The CPNPP, Units 3 and 4, COLA, Revision 3, CSP states:

> The CST monitors and measures the effectiveness and efficiency of the Cyber Security Program and the security controls to ensure that both are implemented correctly, operating as intended, and continuing to provide high assurance that CDAs are protected against cyber attacks up to and including the DBT. Reviews of the security program and controls include, but are not limited to, periodic testing of the security controls, re-evaluation of the capabilities of the adversaries of the DBT, audits of the Physical and Cyber Security Programs and implementing procedures; safety/security interface activities; the Testing, Maintenance, and Calibration Program operating experience; and feedback from the NRC and local, State, and Federal law enforcement authorities.
>
> The insights gained from these analyses are used to:
>
> - Improve performance and effectiveness of the cyber security program,
> - Manage and evaluate risk,
> - Improve the effectiveness of implemented security controls described in Appendices B and C to RG 5.71,
> - Ascertain whether new security controls are required to protect CDAs/CSs from cyber attack,
> - To verify that existing security controls are functioning properly and are effective at protecting CDAs/CSs from cyber attack, and
> - To facilitate corrective action of any gaps discovered in the security program.
>
> The CST verifies the effectiveness of security controls on at least an annual basis or in accordance with the specific requirements for each security control, as

described in Appendices B and C to RG 5.71, whichever is more frequent. The CST reviews records of maintenance and repairs on CDA components to ensure that CDAs which perform security functions are maintained per recommendations provided by the manufacturer.

On the basis of its review of this section, the staff finds that the CPNPP, Units 3 and 4, COLA, Revision 3, CSP appropriately follows the guidance for effectiveness analysis in RG 5.71 and is, therefore, acceptable.

13.8.4.12.4 Vulnerability Assessments and Scans

The CPNPP, Units 3 and 4, COLA, Revision 3, CSP states:

> Luminant's CST conducts periodic vulnerability scanning assessments of the security controls, defensive architecture and of all CDAs to identify security deficiencies. The CST performs assessments of security controls and scans for vulnerabilities in CDAs and the environment at least every 24 months or as specified in the security controls in Appendices B and C to RG 5.71, whichever is more frequent, and when new vulnerabilities that could potentially affect the effectiveness the security program and security of the CDAs are identified. In addition, the CST employs up-to-date vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process.
>
> The Luminant Power CST analyzes vulnerability assessment and scan reports and addresses vulnerabilities that could be exploited to compromise CDAs and vulnerabilities that could adversely impact SSEP functions. The CST shares information obtained from the vulnerability assessment and scanning process with appropriate personnel to ensure that similar vulnerabilities that may adversely impact the effectiveness of the security of interconnected or similar CDAs and/or may adversely impact SSEP functions are understood, evaluated, and mitigated.
>
> Luminant ensures that the assessment and scanning process does not adversely impact SSEP functions. If this should occur, CDAs will be removed from service or replicated (to the extent feasible) before assessment and scanning is conducted. If Luminant cannot conduct vulnerability assessments or scanning on a production CDA because of the potential for an adverse impact on SSEP functions, alternate controls (e.g., providing a replicated system or CDA to conduct scanning) will be employed.

On the basis of its review of this section, the staff finds that the CPNPP, Units 3 and 4, COLA, Revision 3, CSP appropriately follows the guidance for vulnerability assessments and scans in RG 5.71 and is, therefore, acceptable.

13.8.4.12.5 Change Control

The CPNPP, Units 3 and 4, COLA, Revision 3, CSP states:

> Luminant systematically plans, approves, tests, and documents changes to the environment of the CDAs, the addition of CDAs to the environment and changes

> to existing CDAs in a manner that provides a high level of assurance that the SSEP functions are protected from cyber attacks. During the operation and maintenance life cycle phases, the program establishes that changes made to CDAs use the design control and configuration management procedures or other procedural processes to ensure that the existing security controls are effective and that any pathway that can be exploited to compromise a CDA is protected from cyber attacks.

On the basis of its review of this section, the staff finds that the CPNPP, Units 3 and 4, COLA, Revision 3, CSP appropriately follows the guidance for change control in RG 5.71 and is, therefore, acceptable. Further the staff finds that activities described in this section comply with requirements of 10 CFR 73.58, Safety/security interface requirements.

13.8.4.12.6 Configuration Management

The CPNPP, Units 3 and 4, COLA, Revision 3, CSP states:

> Luminant implemented and documented the configuration management controls described in Appendix C, Section 11 to RG 5.71. Luminant implements a configuration and change management process, as described in Section 4.2 of this plan and Section 11 of RG 5.71, to ensure that the site's Cyber Security Program objectives remain satisfied. Luminant ensures that modifications to CDAs are evaluated in accordance with Section 4.2 of this plan before any modification is implemented so as to maintain the cyber security performance objectives articulated in 10 CFR 73.54(a)(1).
>
> During the operation and maintenance phases of a CDA life cycle, Luminant ensures that changes made are conducted using these configuration management procedures to avoid the introduction of additional vulnerabilities, weaknesses, or risks into the system. This process also ensures timely and effective implementation of each security control specified in Appendices B and C to RG 5.71.

On the basis of its review of this section, the staff finds that the CPNPP, Units 3 and 4, COLA, Revision 3, CSP appropriately follows the guidance for configuration management in RG 5.71 and is, therefore, acceptable. Further the staff finds that activities described in this section comply with requirements of 10 CFR 73.58, Safety/security interface requirements.

13.8.4.12.7 Security Impact Analysis of Changes and Environment

The CPNPP, Units 3 and 4, COLA, Revision 3, CSP states:

> Luminant's CST performs a security impact analysis in accordance with Section 4.1.2 [of the CSP] before implementing a design or configuration change to a CDA or when changes to the environment occur so as to manage potential risks introduced by the changes.
>
> Luminant's CST evaluates, documents, and incorporates into the security impact analysis safety and security interdependencies of other CDAs or systems, as well as updates and documents the following:

- The location of the CDA and connected assets,
- Connectivity pathways (direct and indirect),
- Infrastructure interdependencies,
- Application of defensive strategies, including defensive models, security controls, and other defensive strategy measures, and
- Plant-wide physical and cyber security policies and procedures that secure CDAs from a cyber attack, including attack mitigation and incident response and recovery.

Luminant performs these impact analyses as part of the change approval process to assess the impacts of the changes on the security posture of CDAs and security controls, as described in Section 4.1.2 of this plan, and to address any identified gaps to protect CDAs from cyber attack, up to and including the DBT as described in Section 4.2.6 [*of the CSP*].

Luminant manages the cyber security of SSEP functions and CDAs through an ongoing evaluation of threats and vulnerabilities and implementation of each of the security controls provided in Appendices B and C to RG 5.71 during all phases of the life cycle. Additionally, Luminant has established and documented procedures for screening, evaluating, mitigating, and dispositioning threat and vulnerability notifications received from credible sources. Dispositioning includes implementation of security controls to mitigate newly reported or discovered threats and vulnerabilities.

On the basis of its review of this section, the staff finds that the CPNPP, Units 3 and 4, COLA, Revision 3, CSP appropriately follows the guidance for security impact analysis of changes and environment in RG 5.71 and is, therefore, acceptable. Further the staff finds that activities described in this section comply with requirements of 10 CFR 73.58, Safety/security interface requirements.

13.8.4.12.8 Security Reassessment and Authorization

The CPNPP, Units 3 and 4, COLA, Revision 3, CSP states:

Luminant established, implemented, documented, and maintains a process that ensures that modifications to CDAs are evaluated before implementation so that security controls remain effective and that any pathway that can be exploited to compromise the modified CDA is addressed to protect CDAs and SSEP functions from cyber attacks. The program establishes that additions and modifications are evaluated, using a proven and accepted method, before implementation to provide high assurance of adequate protection against cyber attacks, up to and including the DBT, using the process discussed in Section 4.1.2 of this plan.

Luminant disseminates, reviews, and updates the following when a CDA modification is conducted:

- A formal, documented security assessment and authorization policy which addresses the purpose, scope, roles, responsibilities, management commitment, coordination among Luminant entities and compliance to reflect all modifications or additions, and

- A formal, documented procedure to facilitate the implementation of the security reassessment and authorization policy and associated controls.

On the basis of its review of this section, the staff finds that the CPNPP, Units 3 and 4, COLA, Revision 3, CSP appropriately follows the guidance for security reassessment and authorization in RG 5.71 and is, therefore, acceptable.

13.8.4.12.9 Updating Cyber Security Practices

The CPNPP, Units 3 and 4, COLA, Revision 3, CSP states:

Luminant's CST reviews, updates and modifies CPNPP, Units 3 and 4, cyber security policies, procedures, practices, existing cyber security controls, detailed descriptions of network architecture (including logical and physical diagrams), information on security devices, and any other information associated with the state of the security program or security controls provided in Appendices B and C to RG 5.71 when changes occur to CDAs or the environment. This information includes the following:

- Plant- and corporate-wide information on the policies, procedures, and current practices related to cyber security;

- Detailed network architectures and diagrams;

- Configuration information on security devices or CDAs;

- New plant- or corporate-wide cyber security defensive strategies or security controls being developed and policies, procedures, practices, and technologies related to their deployment;

- The site's physical and operational security program;

- Cyber security requirements for vendors and contractors;

- Identified potential pathways for attacks;

- Recent cyber security studies or audits (to gain insight into areas of potential vulnerabilities); and

- Identified infrastructure support systems (e.g., electrical power; heating, ventilation, and air conditioning; communications; fire suppression) whose failure or manipulation could impact the proper functioning of CSs.

On the basis of its review of this section, the NRC staff finds that the CPNPP, Units 3 and 4, COLA, Revision 3, CSP appropriately follows the guidance for updating cyber security practices in RG 5.71 and is, therefore, acceptable.

13.8.4.12.10 Review and Validation Testing of a Modification or Addition of a Critical Digital Asset

The CPNPP, Units 3 and 4, COLA, Revision 3, CSP states:

> Luminant's CST conducts and documents the results of reviews and validation tests of each CDA modification and addition using the process described in Section 3.1.4 of this plan.

On the basis of its review of this section, the staff finds that the CPNPP, Units 3 and 4, COLA, Revision 3, CSP appropriately follows the guidance for review and validation of a modification or addition of a critical digital asset in RG 5.71 and is, therefore, acceptable.

13.8.4.12.11 Application of Security Controls Associated with a Modification

The CPNPP, Units 3 and 4, COLA, Revision 3, CSP states:

> When new CDAs are introduced into the environment, Luminant:
>
> - Deploys the CDA into the appropriate level of the defensive model described in Section 3.1.5 of this plan,
> - Applies the technical controls identified in Appendix B to RG 5.71 in a manner consistent with the process described in Section 3.2 of RG 5.71, and
> - Confirms that the operational and management controls described in Appendix C of RG 5.71 are applied and effective for the CDA.
>
> When CDAs are modified, Luminant:
>
> - Verifies that the CDA is deployed into the proper level of the defensive model described in Section 3.2 of RG 5.71,
> - Performs a security impact analysis, as described in Section 4.2.2 of this plan,
> - Verifies that the technical controls identified in Appendix B to RG 5.71 are implemented in a manner consistent with the process described in Section 3.1.6 of this plan,
> - Verifies that the security controls discussed above are implemented effectively, consistent with the process described in Section 4.1.2 of this plan, and

- Confirms that the operational and management controls discussed in Appendix C to RG 5.71 are applied and effective for the CDA.

On the basis of its review of this section, the staff finds that the CPNPP, Units 3 and 4, COLA, Revision 3, CSP appropriately follows the guidance for the application of security controls associated with a modification in RG 5.71 and is, therefore, acceptable.

13.8.4.12.12 Cyber Security Program Review

The CPNPP, Units 3 and 4, COLA, Revision 3, CSP states:

> Luminant's Cyber Security Program establishes the necessary measures and governing procedures to implement periodic reviews of applicable program elements, in accordance with the requirements of 10 CFR 73.55(m). Luminant reviews the program's effectiveness at least every 24 months. In addition, reviews are conducted as follows:
>
> - Within 12 months of the initial implementation of the program;
> - Within 12 months of a change to personnel, procedures, equipment, or facilities that potentially could adversely affect security;
> - As necessary based upon site-specific analyses, assessments, or other performance indicators; and
> - By individuals independent of those personnel responsible for program implementation and management.
>
> Luminant documents the results and recommendations of program reviews, management's findings regarding program effectiveness, and any actions taken as a result of recommendations from prior program review, in a report to the CPNPP, Units 3 and 4, Senior Vice President and Chief Nuclear Officer at least one level higher than the individual having responsibility for day-to-day plant operation. Luminant maintains these reports in an auditable form, available for inspection, and enters findings from program reviews into the site's Corrective Action Program.

On the basis of its review of this section, the staff finds that the CPNPP, Units 3 and 4, COLA, Revision 3, CSP appropriately follows the guidance for cyber security program review in RG 5.71 and is, therefore, acceptable.

13.8.4.13 Document Control and Records Retention and Handling

The CPNPP, Units 3 and 4, COLA, Revision 3, CSP states:

> Luminant established the necessary measures and governing procedures to ensure that sufficient records of items and activities affecting cyber security are developed, reviewed, approved, issued, used, and revised to reflect completed work. Luminant will retain records and supporting technical documentation required to satisfy the requirements of 10 CFR 73.54 and 10 CFR 73.55,

"Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage," until the NRC terminates the facility operating license. Records required for retention include, but are not limited to, all digital records, log files, audit files, and non-digital records that capture, record, and analyze network and CDA events. These records are retained to document access history and discover the source of cyber attacks or other security-related incidents affecting CDAs or SSEP functions or both. Luminant will retain superseded portions of these records for at least three years after the record is superseded, unless otherwise specified by the NRC.

On the basis of its review of this section, the staff finds that the CPNPP, Units 3 and 4, COLA, Revision 3, CSP appropriately follows the guidance in document control and record retention and handling as described in RG 5.71 and is, therefore, acceptable.

13.8.5 Post-Combined License Activities

As stated in COLA Revision 3, Part 2 FSAR Table 13.4-201, Item 15 the applicant proposed to implement the following license condition in the Security Program:

- **License Condition (13-4)** - Prior to receipt of fuel on-site in the protected area, the Cyber Security Program will be implemented to meet the requirements of 10 CFR 73.54.

The applicant described the CSP and its implementation in accordance with 10 CFR 73.54. The license condition on operational program implementation includes the CSP and its implementation milestones.

In addition, as discussed in Section 13.8.4.3, the staff plans to impose the following license condition below:

- **License Condition (13-5) -** No later than 12 months after issuance of the COL, the licensee shall submit to the Director of the Office of New Reactors a schedule that supports planning for and conduct of NRC inspection of the cyber security program implementation. The schedule shall be updated every 6 months until 12 months before scheduled fuel loading, and every month thereafter until the cyber security program has been fully implemented.

13.8.6 Conclusions

The staff compared COLA, Part 2 FSAR, Chapter 13 ,Section 13.4 and COLA Part 9, Comanche Peak Nuclear Power Plant, Units 3 and 4 Cyber Security Plan to the relevant NRC regulations and the criteria in RG 5.71. On the basis of its review, the staff found that the applicant has adequately addressed STD COL 13.6(1). In addition, the staff finds that the information in the COLA, Revision 3, CSP adequately addresses the relevant requirements and guidance of 10 CFR 73.54, 73.55(a)(1), (b)(8), (m), 73.58 and Appendix G of Part 73. and RG 5.71. Therefore, the staff finds the information contained in this section acceptable.