PMComanchePekNPEm Resource

From: John.Conly@luminant.com
Sent: Friday, July 02, 2010 2:41 PM
To: diane.aitken@dom.com; rjb@nei.org; david.beshear@txu.com; Biggins, James; rbird1@luminant.com; regina.borsh@dom.com; Dennis.Buschbaum@luminant.com; russell_bywater@mnes-us.com; JCaldwell@luminant.com; Ronald.Carver@luminant.com; cp34update@certrec.com; Ciocco, Jeff; Timothy.Clouser@luminant.com; Collins, Elmo; John.Conly@luminant.com; Carolyn.Cosentino@luminant.com; brock.degeyter@energyfutureholdings.com; nancy.douglas@txu.com; Eric.Evans@luminant.com; Rafael.Flores@luminant.com; sfrantz@morganlewis.com; Goldin, Laura; Hamzehee, Hossein; mutsumi_ishida@mnes-us.com; Johnson, Michael; shinji_kawanago@mnes-us.com; kak@nei.org; nicholas_kellenberger@mnes-us.com; Allan.Koenig@luminant.com; Kramer, John; mlucas3@luminant.com; Fred.Madden@luminant.com; Matthews, David; tmatthews@morganlewis.com; Monarque, Stephen; Ashley.Monts@luminant.com; Bill.Moore@luminant.com; ComanchePeakCOL Resource; masanori_onozuka@mnes-us.com; ck_paulson@mnes-us.com; Plisco, Loren; Robert.Reible@luminant.com; jrund@morganlewis.com; jeff.simmons@energyfutureholdings.com; Singal, Balwant; nan_sirirat@mnes-us.com; Takacs, Michael; joseph_tapia@mnes-us.com; Tindell, Brian; Bruce.Turner@luminant.com; Vrahoretis, Susan; Matthew.Weeks@luminant.com; Williamson, Alicia; Willingham, Michael; Donald.Woodlan@luminant.com; diane_yeager@mnes-us.com
Subject: Response to RAI No. 4585 (CP RAI #161)
Attachments: TXNB-10047 RAI 161 (PUBLIC version).pdf

Last week, Luminant submitted the attached response to RAI #161 regarding the physical security of CPNPP Units 3 and 4. The attached letter is the public version of the response. Stephen Monarque and the Document Control Desk each received the SRI version of the correspondence, which included Attachment 3.

If there are any questions regarding the response, please contact me or contact Don Woodlan (254-897-6887, Donald.Woodlan@luminant.com).

Thanks,

John Conly

Luminant
COLA Project Manager
(254) 897-5256

Confidentiality Notice: This email message, including any attachments, contains or may contain confidential information intended only for the addressee. If you are not an intended recipient of this message, be advised that any reading, dissemination, forwarding, printing, copying or other use of this message or its attachments is strictly prohibited. If you have received this message in error, please notify the sender immediately by reply message and delete this email message and any attachments from your system.

Hearing Identifier: ComanchePeak_COL_NonPublic
Email Number: 1909

Mail Envelope Properties (95E7006FD6637C4AAE706E18F8C97B34051E8D78)

Subject: Response to RAI No. 4585 (CP RAI #161)
Sent Date: 7/2/2010 2:41:20 PM
Received Date: 7/2/2010 2:41:53 PM
From: John.Conly@luminant.com

Created By: John.Conly@luminant.com

Recipients:
"diane.aitken@dom.com" <diane.aitken@dom.com>
Tracking Status: None
"rjb@nei.org" <rjb@nei.org>
Tracking Status: None
"david.beshear@txu.com" <david.beshear@txu.com>
Tracking Status: None
"Biggins, James" <James.Biggins@nrc.gov>
Tracking Status: None
"rbird1@luminant.com" <rbird1@luminant.com>
Tracking Status: None
"regina.borsh@dom.com" <regina.borsh@dom.com>
Tracking Status: None
"Dennis.Buschbaum@luminant.com" <Dennis.Buschbaum@luminant.com>
Tracking Status: None
"russell_bywater@mnes-us.com" <russell_bywater@mnes-us.com>
Tracking Status: None
"JCaldwell@luminant.com" <JCaldwell@luminant.com>
Tracking Status: None
"Ronald.Carver@luminant.com" <Ronald.Carver@luminant.com>
Tracking Status: None
"cp34update@certrec.com" <cp34update@certrec.com>
Tracking Status: None
"Ciocco, Jeff" <Jeff.Ciocco@nrc.gov>
Tracking Status: None
"Timothy.Clouser@luminant.com" <Timothy.Clouser@luminant.com>
Tracking Status: None
"Collins, Elmo" <Elmo.Collins@nrc.gov>
Tracking Status: None
"John.Conly@luminant.com" <John.Conly@luminant.com>
Tracking Status: None
"Carolyn.Cosentino@luminant.com" <Carolyn.Cosentino@luminant.com>
Tracking Status: None
"brock.degeyter@energyfutureholdings.com" <brock.degeyter@energyfutureholdings.com>
Tracking Status: None
"nancy.douglas@txu.com" <nancy.douglas@txu.com>
Tracking Status: None
"Eric.Evans@luminant.com" <Eric.Evans@luminant.com>
Tracking Status: None
"Rafael.Flores@luminant.com" <Rafael.Flores@luminant.com>
Tracking Status: None
"sfrantz@morganlewis.com" <sfrantz@morganlewis.com>

Tracking Status: None
"Goldin, Laura" <Laura.Goldin@nrc.gov>
Tracking Status: None
"Hamzehee, Hossein" <Hossein.Hamzehee@nrc.gov>
Tracking Status: None
"mutsumi_ishida@mnes-us.com" <mutsumi_ishida@mnes-us.com>
Tracking Status: None
"Johnson, Michael" <Michael.Johnson@nrc.gov>
Tracking Status: None
"shinji_kawanago@mnes-us.com" <shinji_kawanago@mnes-us.com>
Tracking Status: None
"kak@nei.org" <kak@nei.org>
Tracking Status: None
"nicholas_kellenberger@mnes-us.com" <nicholas_kellenberger@mnes-us.com>
Tracking Status: None
"Allan.Koenig@luminant.com" <Allan.Koenig@luminant.com>
Tracking Status: None
"Kramer, John" <John.Kramer@nrc.gov>
Tracking Status: None
"mlucas3@luminant.com" <mlucas3@luminant.com>
Tracking Status: None
"Fred.Madden@luminant.com" <Fred.Madden@luminant.com>
Tracking Status: None
"Matthews, David" <David.Matthews@nrc.gov>
Tracking Status: None
"tmatthews@morganlewis.com" <tmatthews@morganlewis.com>
Tracking Status: None
"Monarque, Stephen" <Stephen.Monarque@nrc.gov>
Tracking Status: None
"Ashley.Monts@luminant.com" <Ashley.Monts@luminant.com>
Tracking Status: None
"Bill.Moore@luminant.com" <Bill.Moore@luminant.com>
Tracking Status: None
"ComanchePeakCOL Resource" <ComanchePeakCOL.Resource@nrc.gov>
Tracking Status: None
"masanori_onozuka@mnes-us.com" <masanori_onozuka@mnes-us.com>
Tracking Status: None
"ck_paulson@mnes-us.com" <ck_paulson@mnes-us.com>
Tracking Status: None
"Plisco, Loren" <Loren.Plisco@nrc.gov>
Tracking Status: None
"Robert.Reible@luminant.com" <Robert.Reible@luminant.com>
Tracking Status: None
"jrund@morganlewis.com" <jrund@morganlewis.com>
Tracking Status: None
"jeff.simmons@energyfutureholdings.com" <jeff.simmons@energyfutureholdings.com>
Tracking Status: None
"Singal, Balwant" <Balwant.Singal@nrc.gov>
Tracking Status: None
"nan_sirirat@mnes-us.com" <nan_sirirat@mnes-us.com>
Tracking Status: None
"Takacs, Michael" <Michael.Takacs@nrc.gov>
Tracking Status: None
"joseph_tapia@mnes-us.com" <joseph_tapia@mnes-us.com>
Tracking Status: None
"Tindell, Brian" <Brian.Tindell@nrc.gov>

Tracking Status: None
"Bruce.Turner@luminant.com" <Bruce.Turner@luminant.com>
Tracking Status: None
"Vrahoretis, Susan" <Susan.Vrahoretis@nrc.gov>
Tracking Status: None
"Matthew.Weeks@luminant.com" <Matthew.Weeks@luminant.com>
Tracking Status: None
"Williamson, Alicia" <Alicia.Williamson@nrc.gov>
Tracking Status: None
"Willingham, Michael" <Michael.Willingham@nrc.gov>
Tracking Status: None
"Donald.Woodlan@luminant.com" <Donald.Woodlan@luminant.com>
Tracking Status: None
"diane_yeager@mnes-us.com" <diane_yeager@mnes-us.com>
Tracking Status: None

Post Office: MDCTXUEXCL01N4.corptxu.txu.com

Files	**Size**	**Date & Time**
MESSAGE	1134	7/2/2010 2:41:53 PM
TXNB-10047 RAI 161 (PUBLIC version).pdf	1543184	

Options
Priority: Standard
Return Notification: No
Reply Requested: No
Sensitivity: Normal
Expiration Date:
Recipients Received:

WITHHOLD FROM PUBLIC DISCLOSURE UNDER 10 CFR 2.390(d)(1)

Luminant

Rafael Flores
Senior Vice President &
Chief Nuclear Officer
rafael.flores@luminant.com

Luminant Power
P O Box 1002
6322 North FM 56
Glen Rose, TX 76043

T 254.897.5590
F 254.897.6652
C 817.559.0403

CP-201000860
Log # TXNB-10047

Ref. # 10 CFR 52
10 CFR 2.390

June 24, 2010

U. S. Nuclear Regulatory Commission
Document Control Desk
Washington, DC 20555
ATTN: David B. Matthews, Director
Division of New Reactor Licensing

SUBJECT: COMANCHE PEAK NUCLEAR POWER PLANT, UNITS 3 AND 4
DOCKET NUMBERS 52-034 AND 52-035
RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION NO. 4585

Dear Sir:

Luminant Generation Company LLC (Luminant) submits herein the response to Request for Additional Information (RAI) No. 4585 for the Combined License Application for Comanche Peak Nuclear Power Plant Units 3 and 4. This RAI involves the physical security of Units 3 and 4.

Attachment 3 contains security-related information in the responses to two questions and in marked-up FSAR pages. The NRC is requested to withhold Attachment 3 from public disclosure under 10 CFR 2.390(d)(1). This letter is unclassified upon separation from Attachment 3.

Should you have any questions regarding this response, please contact Don Woodlan (254-897-6887, Donald.Woodlan@luminant.com) or me.

The commitments in this letter are captured on page 2.

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

Executed on June 24, 2010.

Sincerely,

Luminant Generation Company LLC

Donald R. Woodlan for

Rafael Flores

Attachments: 1. Response to Request for Additional Information No. 4585 (CP RAI #161) (Public Version)
2. Marked-up FSAR Revision 1 Pages (Public Version)
3. Security Related Information (Withhold from Public Disclsure)

Regulatory Commitments in this Letter

This communication contains the following new or revised commitments which will be completed or incorporated into the CPNPP Units 3 and 4 licensing basis as noted. The Commitment Number is used by Luminant for internal tracking.

Number	Commitment	Due Date/Event
7531	UAP-SGI-08002, High Assurance Evaluation Assessment, will be revised as stated in the response to Questions 13.06.01-25, -27, -28, -33, -34, and -35. (See Note below)	December 31, 2010
7541	(Question 13.06.01-35) - DCD Subsection 13.6.2.6 will be revised to provide consistency in the use of backup and standby power.	Next DCD revision
7551	(Question 13.06.01-4) - Luminant confirms that 10CFR 74.19 recordkeeping requirements will be fully implemented for the possession and storage of Category III SNM prior to receipt of fuel onsite for CPNPP Units 3 and 4 in the protected area.	Prior to receipt of fuel in the protected area
7561	The Security Plan will be revised as stated in the response to Questions 13.06.01-14, -15, -16, -19, -20, -21, -22, -23, -26, -29, -30, -35, -36, -41, -45, -46, -47, -50, and -51. (See Note below)	Next COLA Revision
7571	(Question 13.06.01-27) - UAP-SGI-10003, Rev. 0, will be revised to clearly indicate that the waterborne threat is encompassed in the analysis.	December 31, 2010

Note: the specific content of the commitments is shown in underlined italics in the individual question responses.

Electronic distribution w/all attachments: Stephen Monarque

Electronic distribution w/o attachments:

Rafael.Flores@luminant.com
mlucas3@luminant.com
jeff.simmons@energyfutureholdings.com
Bill.Moore@luminant.com
Brock.Degeyter@energyfutureholdings.com
rbird1@luminant.com
Matthew.Weeks@luminant.com
Allan.Koenig@luminant.com
Timothy.Clouser@luminant.com
Ronald.Carver@luminant.com
David.Volkening@luminant.com
Bruce.Turner@luminant.com
Eric.Evans@luminant.com
Robert.Reible@luminant.com
donald.woodlan@luminant.com
John.Conly@luminant.com
JCaldwell@luminant.com
David.Beshear@txu.com
Ashley.Monts@luminant.com
Fred.Madden@luminant.com
Dennis.Buschbaum@luminant.com
Carolyn.Cosentino@luminant.com
NuBuild Licensing files

Luminant Records Management (.pdf files only)

shinji_kawanago@mnes-us.com
masanori_onozuka@mnes-us.com
ck_paulson@mnes-us.com
joseph_tapia@mnes-us.com
russell_bywater@mnes-us.com
diane_yeager@mnes-us.com
mutsumi_ishida@mnes-us.com
nan_sirirat@mnes-us.com
nicolas_kellenberger@mnes-us.com
rjb@nei.org
kak@nei.org
michael.takacs@nrc.gov
cp34update@certrec.com
michael.johnson@nrc.gov
David.Matthews@nrc.gov
Balwant.Singal@nrc.gov
Hossein.Hamzehee@nrc.gov
Stephen.Monarque@nrc.gov
jeff.ciocco@nrc.gov
michael.willingham@nrc.gov
john.kramer@nrc.gov
Brian.Tindell@nrc.gov
Alicia.Williamson@nrc.gov
Elmo.Collins@nrc.gov
Loren.Plisco@nrc.com
Laura.Goldin@nrc.gov
James.Biggins@nrc.gov
Susan.Vrahoretis@nrc.gov
ComanchePeakCOLResource@nrc.gov
sfrantz@morganlewis.com
jrund@morganlewis.com
tmatthews@morganlewis.com

Attachment 1

Response to Request for Additional Information No. 4585 (CP RAI #161)

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-1

1. **(U)** Part 2 – FSAR, Table 1.8-1R, Significant Site-Specific Interfaces with the Standard US-APWR Design, Interface No. 9 and No. 10 (Page 1.8-7): Luminant is requested to provide reference to Mitsubishi Heavy Industries (MHI) Technical Report UAP-SGI-08002 R1, U.S. APWR - High Assurance Assessment Evaluation Report, that contains descriptions of design and performance requirements for physical protection systems that are a part of the combined license (COL) design and licensing basis for meeting 10 CFR 52.79(a)(35), 52.80(a) and 10 CFR 73.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to provide capabilities to detect, assess, interdict, and neutralize the design basis threat (DBT) and maintain at all time such capabilities. The design of physical protection systems beyond the scope of the design certification (DC) is required as COL Information Item 13.6.1. Title 10 CFR 52.80(a) requires the application to contain information for inspections, tests, and analyses (ITA) and criteria necessary and sufficient to provide reasonable assurance that the facility has been constructed and will operate in conformity with the combined license, the provisions of the Act, and the Commission's rules and regulations. The COL applicant must address interfaces and COL information items for the design of physical protection systems outside the scope of the US-APWR DC.

(U) Interface No. 9 states that "[s]ite security/surveillance systems, such as surveillance cameras, video displays, security detection sensors, communications, access control, etc. Interface is with the standard portion of the site communications system," are identified in the design control document (DCD) as items outside the scope of the standard design. The applicant may conform to guidance of Regulatory Guide (RG) 1.206 for meeting and providing appropriate descriptions for design. The applicant did not reference MHI Technical Report UAP-SGI-08002 contains descriptions of design and licensing bases for physical protection systems for the COL application. Part 8 of the COL application did not provide sufficient descriptions for the detail of design for physical protection systems conforming to guidance of RG 1.206 for a COL application.

(U) Interface No.10 states that "Landscaping features, roadways, walkways, security fences and barricades, and traffic control barriers, etc., that are not part of the standard US-APWR building designs," and "A site arrangement plan is provided in Figure 1.2-1R which shows site-specific features and improvements, as well as the standard US-APWR buildings and features." Figure 1.2-1R, Comanche Peak Units 3 and 4 Site Plan (Sheets 1 and 2) and Figures appearing in MHI Technical Report UAP-SGI-08002 R1 did not provide details, locations, or design for physical protection systems (fences, delays, and barriers) in sufficient design detail that conforms with guidance of RG 1.206 for a COL application.

ANSWER:

The material required by RG 1.206 is included in the Physical Security Plan and additional information from the DCD is incorporated by reference in the FSAR, which includes the High Assurance Evaluation Assessment (HAE) and the Design Certification Physical Security Element Review.

FSAR Subsections 13.6.2 and 13.6.2.2 have been revised to clarify how these documents would be used and maintained for implementation of the Security Plan. The revisions clarify the distinction between the "Security Plan" and the security programs that implement the "Security Plan."

FSAR Subsection 13.6.2 has been revised to clarify that Appendix A to the HAE describes the capability of the US-APWR design (including the reference plant descriptions which are the physical protection systems and design features for CPNPP, the reference plant for these assessments) to meet the performance requirements of 10 CFR 73.55(b) up to and including the time of COL issuance for CPNPP Units 3 and 4 and that continued high assurance performance for CPNPP Units 3 and 4 is maintained and is described in plant specific supporting documents including design documents, procedures and records. FSAR Subsection 13.6.2.2 has been revised to show how the Design Certification Physical Security Element Review would be used and maintained.

The continued high assurance after issuance of the COL for CPNPP Units 3 and 4, including the protective strategy and the physical security features design and performance requirements, will be maintained in plant procedures and other plant-specific supporting documents and records. This approach is in accordance with the NRC's physical security regulations in 10 CFR 73, Appendix C, II.B.5.c.(v).

FSAR Section 13.6 is referenced in Interface #9 of FSAR Table 1.8-1R and the HAE Report is referenced in Section 13.6. Therefore, it is not necessary to add a reference to the HAE Report in Interface #9.

Regarding Interface #10 of FSAR Table 1.8-1R, the site arrangement plan in Figure 1.2-1R provides the level of detail currently available for the site arrangement plan. Also, see the responses to Questions 13.06.01-6, -28, and -29 below for additional information regarding security features external to the standard plant.

<u>Impact on R-COLA</u>

See attached marked-up FSAR Revision 1 pages 13.6-1, 13.6-2, and 13.6-3 (all SRI).

<u>Impact on S-COLA</u>

None.

<u>Impact on DCD</u>

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-2

2. **(U)** COL Part 2 – FSAR, Table 1.8-201, Resolution of Combined License Items for Chapter 1-19,, Pages 50 – 52 and 54): Luminant is requested to provide a summary of how COL 13.3(4), "The COL Applicant is to develop the security-related aspects of emergency planning" was addressed in the Comanche Peak Nuclear Power Plant (CPNPP), Units 3 and 4 COL Application Part 5 "Emergency Plan."

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for combined license (COL) include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. The DCD Tier 2 COL Information COL 13.3(4) is intended to ensure that applicant address the interfaces between programs and plans for implementing emergency response. COL Application Part 2, FSAR, Chapter 13.3, Emergency Planning, states that, "[e]mergency classification and action levels, but the security-related aspects of the emergency planning are addressed in the CPNPP Units 3 and 4 Combined License Application Part 5 "Emergency Plan," and did not describe what security-related considerations are appropriate or needed.

(U) Clarification is requested of how (or what) security-related aspects of emergency planning are required to be addressed in the emergency plan to adequately fulfill the stated COL information item (e.g., support, interfaces, and reliance on security programs and contingency response plan, support of emergency response organization, coordination during events, communications, access controls for emergencies, etc.).

(U) Note: The information addressing specific details related to security features or providing security functions will be safeguards information (SGI) and should be marked and protected in accordance with 10 CFR 73.21. The applicant should portion mark text in the response to request for additional information (RAI) as appropriate to identify SGI (or Official-Use-Only Security-Related Information) that reveals the specific details of physical protection.

ANSWER:

The Emergency Plan (EP) fully integrates security-related events, security response, and coordination between security personnel and plant safety personnel in its treatment of a wide range of emergency conditions that are postulated for the site. Specifically, the security-related aspects of the EP include the following:

- interactions between the Security and Emergency Planning staffs
- the role of the Security Coordinator on the Plant's Emergency Operations Team
- the role Security personnel play in a safety-related emergency, including access control and personnel accountability
- how a variety of security threats are treated as anticipated EP events
- the roles played by Security personnel in various EP Alert Levels
- the communications systems used by Security and EP personnel to coordinate emergency operations
- the role played by local law enforcement in a variety of EP scenarios
- the role of the Security organization in site evacuations
- the elements of Security training that deal with emergency operations
- the role of Security personnel in notifying plant personnel of emergency conditions
- communications between the Security Shift Supervisor, the CAS, SAS, and the Control Room during emergencies
- The relationship between security events and Emergency Action Levels (EALs)

Impact on R-COLA

None.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-3

3. **(U)** Part 2 – FSAR, Chapter 13, Section 13.1.1.2.1, CPNPP Units 3 and 4 Site Organization, Review Committee (3rd bullet, Page 13.1-3): Clarify whether the "Operations Review Committee (ORC) and the Station Operations Review Committee (SORC)" are applicable for independent reviews of activities affecting plant security during operations for managing safety/security interface.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for combined license (COL) include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.58 states that each licensee shall assess and manage the potential for adverse effects on safety and security, including the site emergency plan, before implementing changes to plant configurations, facility conditions, or security. The applicability of review committees to provide independent reviews of activities affecting plant security should be specified. The applicant did not include descriptions or reference specifics descriptions in COL Part 2 that address the requirements of 10 CFR 73.58. The descriptions in Part 8, Physical Security Plan, Section 17, Review, Evaluation and Audit of the Physical Security Program, did not adequately address how applicant will manage and plans to implement safety/security interface in accordance with NRC regulation. Section 17 of the security plan only addresses reviews and audits of program no longer than 12 months after changes.

ANSWER:

See the response to Question 13.06.01-18 below.

Impact on R-COLA

See attached marked-up FSAR Revision 1 page 13.1-3.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-4

4. **(U)** Part 2, Table 13.4-201, Operational Programs Required by NRC Regulations and Program Implementation, Item 15 (Page 13.4-7): Confirm the intent to fully implement physical protection requirements (i.e., all physical protection systems and operational programs) of an operating reactor in accordance with 10 CFR 73, including Appendix B and Appendix C, "prior to receipt of fuel on-site," as stated in Item 15 of proposed license conditions and implementation milestones. In addition, confirm and indicate in the COL application that requirements of 10 CFR 74.19, Recordkeeping, will be implemented for the possession and storage of Category III SNM. .

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Item 15 of the proposed license conditions and milestones requires full implementation of the Physical Security Program, Safeguards Contingency Program, and Training and Qualification Program, prior to initial receipt of fuel. Title 10 CFR 73.67, "Licensee fixed site and in-transit requirements for the physical protection of special nuclear material of moderate and low strategic significance, may be applied for protection to storage of Category III reactor fuel assemblies, along with 10 CFR Part 74, "Material Control and Accounting of Special Nuclear Material," and security enhancements requirements that followed the events of 9/11 (i.e., NRC Orders to Cat III fuel cycle licenses) are current regulatory requirements for physical protection for the possession of Category III special nuclear material (SNM). Appropriate physical protection commensurate with Category III material may be applied based on NRC Regulatory Guide 5.76, with appropriate application regulatory requirement for processing request for exemption in accordance with 10 CFR Part 73.55(a)(4). Title 10 CFR 74.19 requires recordkeeping for special nuclear material of low strategic significance nuclear material for licensee not subject to 10 CFR 74.31 (i.e., utilization facility licensed pursuant to Part 50 or 70). Confirmation and a commitment are needed to ensure the Part 52 licensee will apply the same requirements for material control and accounting at the receipt of fresh fuel.

ANSWER:

In FSAR Table 13.4-201, Luminant established a license condition which confirms that all physical protection and security-related operational programs will be fully implemented in accordance with 10 CFR 73 (including all applicable appendices) prior to receipt of fuel on-site. FSAR Table 13.4-201, Item 15, has been revised to more clearly identify the milestones for the security program as "Prior to receipt of fuel on–site for CPNPP Units 3 and 4 (in the protected area)."

Luminant confirms that 10CFR 74.19 recordkeeping requirements will be fully implemented for the possession and storage of Category III SNM prior to receipt of fuel onsite for CPNPP Units 3 and 4 in the protected area.

Impact on R-COLA

See attached marked-up FSAR Revision 1 pages 13.4-7 and 13.4-8.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-5

5. **(U)** Part 2, Section 13.5.1.2, Preparation of Procedure, Plant Security Procedures (page 13.5-6) and Section 13.6, Security (1st paragraph, Page 13.6-1): Describe the management controls for ensuring "information concerning specific design features and administrative provisions of the security plan" will be protected to limit access to only individuals with "a need-to-know basis." Specifically, describe the requirements for management and administrative controls (e.g., policies, processes, and procedures) that will be established for protection of safeguards information in accordance with requirements of 10 CFR 73.21 during constructions and operations of the CPNPP Units 3 and 4.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73. Security systems and procedures that are considered safeguards information are required to be protected in accordance with requirements of 10 CFR 73.21. Security plans submitted under Part 8 of the COLA did not describe how program will be established to meet requirements of 10 CFR 73.21. As an applicant, Luminant has established an acceptable management and administrative controls for meeting 10 CFR 73.21 for preparing COL application. However, the COL application did not include plans to apply similar or appropriate management controls required for construction (e.g., information on security systems, features, and hardware design, construction, and installation) and operations phases of the CPNPP, Units 3 and 4.

ANSWER:

CPNNP Units 1 and 2 have a safeguards information protection program in accordance with 10 CFR 73.21. The management and administrative controls for the protection of safeguards information for Units 3 and 4, including the dissemination of information in accordance with the "need-to-know" principle, will be identical to the policies, processes, and procedures that are in use at CPNPP Units 1 and 2. The CPNPP Unit 1 and 2 operational program for control of Safeguards Information is attached. This procedure is typical of how this program would be implemented for CPNPP Units 3 and 4.

Attachment

STA-308, "Control of Safeguards Information"

Impact on R-COLA

None.

Impact on S-COLA

None.

Impact on DCD

None.

COMANCHE PEAK NUCLEAR POWER PLANT

STATION ADMINISTRATION MANUAL

PROTECTION OF SAFEGUARDS INFORMATION and SAFEGUARDS INFORMATION - MODIFIED

PROCEDURE NO. STA-308

REVISION NO. 12

SORC MEETING NO.: 09-004 DATE: 2-24-09

EFFECTIVE DATE: 3-05-09

ELECTRONIC CONTROLLED COPY

CHANGES ARE NOT INDICATED

LATEST CHANGE NOTICE EFFECTIVE DATE _____/_____

Verify current status in the Document Control Database prior to use.

PREPARED BY (Print):	Neil Harris	EXT.	5449
TECHNICAL REVIEW BY (Print)	Herb Kenyon	EXT.	6382
APPROVED BY:	Dave Kross	DATE:	02/25/09

PLANT MANAGER

1.0 PURPOSE

The purpose of this procedure is to prescribe methods and define responsibilities for the handling and protection of Safeguards Information (SGI) including Safeguards Information -Modified (SGI-M).

2.0 APPLICABILITY

This procedure applies to those organizations and individuals associated with the Comanche Peak Steam Electric Station (CPNPP) who receive, produce, or acquire Safeguards Information. Specific guidance is provided concerning: access, storage, marking, destroying, reproducing, and transmitting Safeguards Information including Safeguards Information -Modified. Throughout the procedure, actions associated with SGI should also apply to SGI-M.

3.0 REFERENCES

3.1 Title 10 of the Code of Federal Regulations (10CFR), Parts 2.790 (d); 73.2; 73.21, 73.22, 73.23 and 73.57.

3.2 NRC Generic Letter 87-10, "Implementation of 10CFR 73.57, Requirements for FBI Criminal History Checks."

3.3 NUREG-0794, "Protection of Unclassified Safeguards Information," October 1981.

3.4 NRC Regulatory Issue Summary 2002-15, 08/28/2002.

3.5 CPNPP Procedure STA 421, "Initiation of Smartforms".

3.6 CPNPP Procedure STA-902, "Access to CPNPP Site Areas"

4.0 DEFINITIONS/ACRONYMS

4.1 Authorized Individual

4.1.1 An individual (1) whose FBI fingerprint results have been appropriately evaluated,(2) considered trustworthy and reliable and (3)who has a current need to know for the Safeguards Information.

4.1.2 Employees, contractors, and agents of the Nuclear Regulatory Commission (NRC), the United States government, or the International Atomic Energy Agency; members of authorized congressional committees; the Governor of the state or designated representatives; and members of state or local law enforcement agencies.

4.2 Safeguards Information (SGI)

Information which specifically identifies CPNPP' detailed security measures for the physical protection of Special Nuclear Material and security measures for the physical protection and location of certain plant equipment vital to the safety of production or utilization facilities. Specific categories of Safeguards Information are described in Attachment 8.A.

4.3 Need to Know

A determination by a person having responsibility for protecting SGI that a proposed recipient's access to SGI is necessary in the performance of official, contractual, or licensee duties of employment.

4.4 Safeguards Information Storage Containers - includes any of the following repositories:

4.4.1 A steel filing cabinet equipped with a steel locking bar secured by a General Services Administration (GSA) approved padlock. For filing cabinets to be acceptable they should be: (1) inside the Protected Area or (2) if outside the Protected Area, in a building where personnel access is controlled during business hours, the building is locked at night and the location approved by the Security Manager.

4.4.2 A security filing cabinet (safe) that bears a test certification label on the locking drawer, or interior plate, that is marked "General Services Administration Approved Security Container" on the exterior of the top drawer or door (GSA Class 6 container).

4.4.3 Other repositories, such as vaults or vault type rooms, which provide comparable physical protection in the judgement of the NRC.

4.5 Safeguards Information-Modified Storage Containers

4.5.1 When unattended, SGI-M must be stored in a locked file drawer or cabinet which the knowledge of the lock combination or access to keys is limited to a minimum number of personnel who have a 'need to know' and are otherwise authorized access.

4.6 Pretty Good Privacy (PGP)

An application and protocol for secure e-mail and file encryption. The use of protected electronic communications for transmittal of SGI allows efficient exchange of encrypted information between licensees, NRC, and NEI enabling more effective administration and control of security programs.

4.7 Key pair

Consists of a public key, which encrypts data, and a private key, for decryption.

4.8 Pass-phrase

A pass-phrase is a longer version of a password and provides more security to the program.

4.9 Security Field Report

A Security form used to document Security related events and Smartform (SMF) activities that contain SGI (e.g. unattended SGI, signs of tampering, equipment problems, serious contingency events, and minor traffic accidents) or SGI-M related events.

4.10 Safeguard Information-Modified

Safeguards Information-Modified associated with Category1 or 2 'Quantities of Concern' materials as identified in 10CFR 73.23 and other information and matter as determined by the Commission.

4.11 Trustworthy and Reliable

Trustworthy and Reliable are characteristics of an individual considered dependable in judgement, character and performance and does not constitute an unreasonable risk to public health and safety or common defense and security. Such determination is based upon a background check.

5.0 RESPONSIBILITIES

5.1 Luminant Power Security Manager (CPNPP)

5.1.1 Responsible for the overall implementation of the Safeguards Information Program for Comanche Peak Nuclear Power Plant (CPNPP).

5.1.2 Responsible for the final determination as to whether or not material is Safeguards Information.

5.1.3 Responsible for maintaining this procedure current.

5.1.4 Responsible for ensuring that fingerprints are submitted to the FBI for all personnel requiring access to Safeguards Information and for ensuring that the resulting criminal history checks are appropriately evaluated.

5.1.5 Responsible for the SGI encryption program.

5.1.6 Responsible for ensuring individuals have appropriate user level knowledge of encryption software prior to being granted permission to encrypt and electronically transmit SGI.

5.1.7 Responsible for granting individual permission to use encryption software, transmit SGI, and maintain a list of authorized users.

5.1.8 Responsible for ensuring all holders of a public key are notified if a pass-phrase, key pair has been or is suspected of being compromised.
[27316]

5.1.9 The Security Manager can delegate any of the responsibilities noted above to a Security Supervisor for performance and implementation.

5.2 Organizational Primary Designee (OPD)

An individual designated by a department manager as responsible for ensuring that the requirements for protecting SGI or SGI-M are implemented, as applicable to the respective department, in accordance with this procedure.

5.3 Authorized SGI Encryption User

5.3.1 Responsible for the use of encryption software and has demonstrated the ability to properly use it.

5.3.2 For each assigned public key, maintain a user Authorized SGI Encryption User List (form STA 308-2) and a Public Key Distribution Log (form STA-308-3) of individuals who have been provided a copy of the public key.

5.3.3 Collect, store, and handle all company private keys as SGI.

5.3.4 Responsible for reporting to the Security Manager when a pass-phrase, key pair, or electronic file has been, or is suspected of being compromised.

5.3.5 Normally, the encryption software (PGP) user is a member of Security or Regulatory Affairs. Other organizations may be evaluated for use of PGP on a need bases and approved by the Security Manager or Security Supervisor.

6.0 INSTRUCTIONS

6.1 Safeguards Information Protection Programs

Each organization that receives, produces, or acquires material containing SGI or SGI-M shall ensure compliance with the protection requirements of this procedure. Safeguards Information and Safeguards Information-Modified programs should also incorporate the following provisions:

6.1.1 Each manager whose organization receives, produces or acquires material containing SGI should identify to Security, Organizational Primary Designees (OPD's) within the department who are responsible for ensuring that SGI is protected in accordance with this procedure.

6.1.2 Each organization which implements the SGI Program should be subject to unannounced review by a representative of the Security organization.

6.1.3 When questions arise about a possible SGI category, the Security Manager or his designee makes the final determination.

6.1.4 In order to facilitate inter-department work involving SGI documents, the Security Manager may establish an informal list of individuals who are authorized continuous access to SGI or SGI-M. The list should contain the names of personnel who have a permanent or regular need for access to SGI or SGI-M, as determined by the various managers.

6.1.4.1 Individuals may be placed on this list by their respective managers by notifying the Security Manager of the need. Personnel should be removed in the same manner when the need no longer exists.

6.1.4.2 Other individuals, not included on this list, who meet the requirements of Section 4.1, should still be granted access to SGI when necessary.

6.1.4.3 Individuals needing access to SGI or SGI-M who do not have current unescorted access authorization should be processed in accordance with STA-902 to ensure the necessary elements of an Authorized Individual are met prior to being granted access.

6.1.5 In order to facilitate inter-department work involving SGI-M documents, the documents may be sent either as hard copy or electronically meeting the same level of protection afforded SGI. However, hard copy or electronic media containing SGI-M may be double enveloped (unmarked outer envelope) and placed in locked drawers or containers when not in use. Electronic documents may be stored on hard-drives, thumb-drives or other electronic media. CDs or other portable electronic media shall be marked "Safeguards Information-Modified".

6.2 Safeguards Information and Safeguards Information-Modified Protective Measures

The following protective measures shall be utilized by each organization which implements the SGI Program and compliance should be ensured by the Organizational Primary Designees.

6.2.1 Access Control

6.2.1.1 No person shall have access to SGI material unless the individual is authorized as defined in Section 4.1.

6.2.1.2 When SGI is being given to, transferred to, or transmitted to an authorized recipient, the authorized recipient shall be informed that SGI is involved.

6.2.1.3 OPD's shall ensure that authorized recipients who receive SGI are aware of their responsibilities for protecting the information in accordance with this procedure.

6.1.1.4 Individuals using SGI-M shall be considered trustworthy and reliable. Information reviewed is not in the public domain and should not be transferred to individuals external of those organizations using the SGI-M. Access to SGI-M is in accordance with authorization per Section 4.1.

6.2.2 Marking of Documents

6.2.2.1 Each document or other matter that contains SGI / SGI-M shall have on the face of the document (1) the name, title, and organization of the individual authorized to make a SGI determination and who has determined that the document contains SGI, (2) the date the document was originated or the determination made, (3) an indication that the document contains SGI, and (4) an indication that unauthorized disclosure would be subject to civil and criminal actions. This determination information is only required on the first page of a multi page document.

6.2.2.2 The determination stamp is not required on documents which do not contain original SGI / SGI-M, such as work requests, Security Field Reports, audit reports, etc.

6.2.2.3 Each page of a SGI document shall be marked in a conspicuous fashion at the top and bottom with the statement "Safeguards Information" or "Safeguards Information-Modified" as applicable.

6.2.2.4 Transmittal letters or memoranda which accompany Safeguards documents, but do not in themselves contain SGI / SGI-M, shall be marked to indicate that attachments or enclosures contain SGI / SGI-M or attached to a cover sheet that identifies the package as containing SGI / SGI-M.

6.2.2.5 Documents and correspondence that contain SGI / SGI-M, in addition to the information required on the face of the document, shall be marked to indicate which portions (e.g., paragraphs, pages, or appendices) contain SGI / SGI-M and which do not.

6.2.2.6 Documents, correspondence and other matter shall be marked on each page; " Safeguards Information-Modified" or "SGI-M" at the top of each page. This includes any documents sent as electronic media. The bottom of each page shall be marked "Safeguards Information-Modified".

6.2.3 Control/Storage of Safeguards Information and Safeguards Information-Modified

6.2.3.1 SGI, when not in use, shall be kept locked in a security container. Knowledge of container lock combinations shall be kept to the minimum number of personnel authorized access.

6.2.3.2 Combinations to Safeguards repositories should be changed annually, and or, when an individual no longer has authorized access to the repository combination.

6.2.3.3 SGI and SGI-M shall be protected while in use. This requirement is met if the material is being attended when it is not actually being utilized. SGI material in Security alarm stations or continuously manned Security posts, is not required to be kept locked in security containers. Additionally, Security instructions and procedures may be posted as long as they are protected from public view. This general protection policy is extended to administrative offices, engineering, and drafting areas, if visitors are escorted, and to certain Vital Areas such as the Control Room.

In addition to the Human Performance Tool - Self Check (Stop, Think, Act and Review or STAR), one or more of the following techniques or tools should be used when SGI is removed from SGI containers:

Flashing Lights
Conspicuous folder and/or paper
Peer Checking

6.2.3.4 Upon removal of SGI from a safeguards material container, the container should be secured. The container can remain open if the controlling individual (user) is aware of the open container and remains in the area where they can continuously observe said container. If the SGI user needs to leave the area and leave the container open, the user can be relieved by another individual meeting the requirements for SGI access. Repositories/containers

should be checked to ensure that they are locked, if the area will be unattended, and at the end of the work day.

6.2.3.5 SGI-M storage does not require the same level of protection afforded SGI. However, hard copy or electronic media containing SGI-M may be double enveloped (unmarked outer envelope) and placed in locked drawers or containers when not in use. Electronic documents may be stored on hard-drives, thumb-drives or other electronic media and stored in the same manner.

6.2.4 SGI Transmittals

6.2.4.1 When transmitted outside of an authorized place of use or storage, SGI material shall be placed in an envelope or wrapper which is marked with the intended recipient's name and address and marked on both sides, top and bottom, "Safeguards Information."

6.2.4.2 This envelope or package shall be placed in another envelope or package which shall be routinely addressed. No Safeguards marking shall be placed on the external envelope or package.

6.2.4.3 Such material may be transmitted by messenger, U.S. First Class, Registered, Express, Certified Mail, or by any person authorized access to the information. Unattended SGI material, scheduled for transit, shall be maintained in approved containers until placed into an authorized transmittal process and shall not be stored in desk drawers or other type of unapproved containers.

6.2.4.4 When individuals transport SGI, they shall retain the SGI material in their personal possession at all times and shall not leave it in automobiles, hotel/motel rooms or safes, private homes, or in the possession of unauthorized individuals.

6.2.4.5 Transmittal of SGI-M should be limited to only those who specifically need the information, understand the controls necessary and meet Section 4.1 requirements. This does not preclude others from reviewing the information but care should be taken to assure trustworthiness and reliability of the persons receiving the information. Transmittal of SGI-M may be performed by placing in an unmarked folder or electronic documents may be transmitted on hard-drives, thumb-drives or other electronic media using password protection.

6.2.5 Destruction of Safeguards and Safeguards Information-Modified Documents

If SGI or SGI-M needs to be destroyed, OPD's should accomplish this action, or ensure that it is accomplished by an authorized individual. The material shall be destroyed by tearing into small pieces (piece sizes ½ inch or smaller) and mixing with pieces of other pages, burning, shredding, or by any other means that prevents reconstruction by means available to the general public.

6.2.6 Reproduction of Safeguards Documents

SGI shall be reproduced to the minimum extent necessary. The recipient shall be an authorized individual as defined in Section 4.1 and is responsible for protecting the material as required by this procedure.

6.2.7 Reproduction of Safeguards Information-Modified Documents or Electronic Media

SGI-M should be reproduced to the minimum extent necessary. Recipients should be authorized per Section 4.1, however, This does not preclude others from reviewing the information but care should be taken to assure trustworthiness and reliability of the persons receiving the information and understands the requirements of controlling the documents.

6.3 Communications

6.3.1 SGI shall not be transmitted by unprotected communications circuits, except under emergency or extraordinary circumstances, such as conditions that require immediate communications in order to respond to a Safeguards event. This restriction applies to telephone, telegraph, teletype, facsimile circuits, radio, and electronic mail or transfer. SGI that has been encrypted with PGP maybe transmitted by unprotected communications circuits.

6.3.1.1 Routine telephone or radio transmissions between the Security Organization and local police shall be limited to message formats or codes that do not disclose site safeguards features or response procedures.

6.3.1.2 Infrequent or non-repetitive telephone conversations regarding the CPNPP Security Plan or implementing procedures are permitted, providing the discussion is of a general nature or the identification of SGI is disguised.

6.3.2 SGI or SGI-M shall not be discussed openly in public in order to prevent unauthorized access. When meetings or hearings are conducted and SGI or SGI-M is to be discussed, OPD's or Security personnel shall ensure that all personnel present are authorized to receive the information. All two-way pagers, cell

phones, two-way radios shall be turned off when discussing SGI or SGI-M. Transcripts or minutes of meetings or hearings containing SGI shall be protected accordingly.

6.4 Electronic Data

6.4.1 Electronic Data Processing Equipment (EDPE)

Reproduction and hard copy printing of SGI and SGI-M may be processed or produced using printers, scanners, copiers and /or any electronic data processing equipment with memory capability providing all recorded information is promptly removed from the equipment.

Note: Paragraph 6.2.3.3 (protection of SGI while in use) applies to electronic data processing equipment, including computers.

6.4.2 SGI that is produced and processed on a computer or word processor should meet one or both of the following:

6.4.2.1 SGI should be produced, processed and stored on a dedicated computer (e.g. laptop) that is self contained and is not connected to a networking system (LAN) or is approved by the NRC. When unattended or not in use the computer shall be stored as SGI in accordance with this procedure, i.e. SGI, when not in use, shall be kept locked in a security container.

6.4.2.2 SGI should be produced and processed on a dedicated PC that is self contained (disconnected / disabled from any networking system) and has a removable SGI designated hard drive or is approved by the NRC. An SGI designated hard drive should contain a bootable operating system which should be used to initialize the computer. The SGI designated hard drive should also contain the software application programs necessary to process the SGI data. Data should be processed and saved on the same SGI designated hard drive. When unattended the SGI hard drive shall be stored in accordance with this procedure, i.e. SGI, when not in use, shall be kept locked in a security container.

Note: These systems shall be self contained so that only the individual working on the system has access to the SGI files.

6.4.3 SGI and SGI-M should only be copied on those copy machines approved for safeguards copying. Those machines not acceptable for safeguards copying are labeled "Do not scan or copy safeguards information on this equipment". If a user believes a copy machine's acceptability is indeterminate, they should not use it and contact Administrative Services.

6.4.4 The basic objective of the electronic data requirements is to ensure that

unauthorized individuals can not obtain access and retrieve SGI or SGI-M from computers and EDPE, particularly from remote terminals.

6.4.5 Encryption software allows designated users to encrypt, decrypt, manage, and electronically transmit and receive sensitive security information via telephone or data link lines. Once an electronic document has been encrypted with PGP it may be transferred to a network connected computer and transmitted electronically to authorized recipients.

6.5 Removal from Safeguards Information Category

6.5.1 Documents should only be removed from the SGI category either by, or with the permission of, the individual (or office) who made the original determination or by the Security Manager. The Security Manager should be notified prior to the documents being removed.

6.5.2 At a minimum, documents shall be marked on the first page with the name and organization of the individual who removed the documents from the SGI category and the date of removal.

6.5.2.1 Documents containing 2 pages or less should be declassified by placing a stamp on the first page, with the above information filled in, and lining through the protective markings on subsequent pages.

6.5.2.2 Documents containing 3 pages or more may be declassified by using a Safeguards Information Declassification Cover Sheet (form STA-308-1) attached to the front of the document. Documents declassified in this manner do not require the protective markings to be lined through, unless pages are separated from the package.

6.5.2.2.1 Protective markings on separate pages, should be lined through, upon separation from the SGI Declassification Cover Sheet, by the individual removing the pages.

6.5.2.2.2 Although not required, documents that are declassified using a Safeguards Information Declassification Cover Sheet may have all the protective markings lined through.

6.5.3 The Security Manager or his designee should initiate notification to all of the OPD's when he approves material to be removed from the SGI category.

6.5.4 SGI should be reviewed on an as needed basis, determined by the Security Manager or his designee , for declassification of documents no longer requiring SGI status.

6.5.5 Documents originally containing SGI shall be removed from the SGI category whenever the information no longer meets the SGI criteria.

6.6 Reports of Violations

Any incident concerning the misuse, mishandling, loss, theft, misplacement, or lack of protection of SGI or SGI-M should be reported to the Security Manager immediately. The Security Manager should ensure that an investigation of the incident is conducted, initiate required notifications, and should initiate a Smartform in accordance with STA-421. The Smartform should not contain any actual SGI or SGI-M, but should provide sufficient information to summarize the incident and allow for tracking and trending (e.g. safeguards left unattended) details are recorded on a Security Field Report (SFR).

6.7 Training

6.7.1 Organizational Primary Designees and authorized recipients should be aware of all protection requirements for SGI. Training for awareness of current requirements should be accomplished via information provided in Plant Access Training, review of this procedure and other media identified by Security.

6.7.2 Further training for OPD's shall be provided, if necessary to ensure that the protection of SGI is followed for the respective departments, as determined by the Security Manager. [26934]

6.8 Official Use Only -Security Related Information

A lower tier type of information regarding the physical protection of nuclear materials and facilities or information concerning material control and accounting for Special Nuclear Material or other information deemed as having protective requirements but not classified as either SGI or SGI-M may be produced. This information is not subject to the bulk of protective requirements and may be disseminated with the knowledge that the information is not to be shared with the public or individuals that do not have a need to know.

Such information has been generically deemed by the NRC to be confidential and to be withheld from public disclosure under exemption from the Freedom of Information Act. Documents or correspondence submitted to or received from the NRC, other agencies or third parties that contain such information should be marked to contain 10CFR2.390(d)(1) type information. This information may be transmitted electronically or in hard copy without being encrypted or protected in other manners. This information should be moved from email accounts as soon as it has been stored electronically and/or printed.

7.0 FIGURES

None

8.0 ATTACHMENTS/FORMS

8.1 Attachments

8.A Attachment 8.A, "Types of Safeguards and Non-Safeguards Information"

8.2 Forms

8.2.1 STA-308-1, "Safeguards Information Declassification Cover Sheet"

8.2.2 STA-308-2, "Authorized SGI Encryption User List"

8.2.3 STA-308-3, "Public Key Distribution Log"

9.0 RECORDS

None

ATTACHMENT 8.A
PAGE 1 OF 3

TYPES OF SAFEGUARDS and NON-SAFEGUARDS INFORMATION

SAFEGUARDS INFORMATION (SGI)

(1) The CPNPP Security Plan in its entirety.

(2) CPNPP specific drawings, sketches or maps that substantially represent the final design features of the physical protection system.

(3) Details of alarm system layouts showing location of intrusion detection devices, alarm assessment equipment, alarm system wiring, emergency power sources, and duress alarms.

(4) Written physical security orders and procedures for members of the Security Organization, that indicate duress codes and patrol schedules when specific response times and routes are identified.

(5) Details of on-site and off-site communications systems that are used for security purposes.

(6) Lock combinations and mechanical key designs.

(7) Documents and other matter that contain lists or locations of certain safety-related equipment explicitly identified as vital for purposes of physical protection as contained in the CPNPP Security Plan, Safeguards Contingency Plan, or plant specific safeguards and analyses.

(8) The composite Safeguards Contingency Plan for CPNPP.

(9) Those portions of the CPNPP Security Training and Qualification Plan which disclose features of the physical security system or response procedures.

(10) Response plans to specific threats detailing size, disposition, response times and armament of responding forces.

ATTACHMENT 8.A
PAGE 2 OF 3

TYPES OF SAFEGUARDS and NON-SAFEGUARDS INFORMATION

(11) Size, armament and disposition of on-site reserve forces.

(12) Size, identify or armament, and arrival times of off-site forces committed to respond to safeguards emergencies.

(13) Information not otherwise classified as National Security Information or Restricted Data relating to safeguards inspections and reports. Specifically: Portions of safeguards inspection reports, evaluations, audits, or investigations that contain details of the CPNPP physical security system or that disclose uncorrected defects, weaknesses, or vulnerabilities in the system. Information regarding defects, weaknesses, or vulnerabilities may be released after corrections have been made. Reports or investigations may be released after the investigation has been completed unless withheld pursuant to other authorities; e.g., The Freedom of Information Act (5 USC 552).

(14) PGP private key(s) and pass-phrase(s), used to produce, receive, or acquire SGI material.

(15) Portions of correspondence insofar as they contain SGI specifically defined in Attachment 8.A.

SAFEGUARDS INFORMATION - MODIFIED

(9) Information controlled as Safeguards Information-Modified (SGI-M). This information includes amounts of Category I and II radiological materials on site and/or being shipped off site.
(10) Engineering and safety analyses, security related procedures or scenarios revealing site specific details of the facility .
(11) Information deemed SGI-m by the NRC or other agency.

NON-SAFEGUARDS MATERIAL

To assist in identifying SGI it is necessary to explain that certain material may seem to meet the criteria but, does not fall within the scope of the rule for identifying SGI Information. Examples of types of material not included are:

(1) Generic studies, reports, or analyses conducted by, or on behalf of, the NRC, licensees, or applicants which concern the safeguarding of nuclear materials or facilities.

ATTACHMENT 8.A
PAGE 3 OF 3

TYPES OF SAFEGUARDS and NON-SAFEGUARDS INFORMATION

(2) Documents, drawings, or reports submitted by license applicants, licensees or produced by the NRC in response to the Environmental and Safety Requirements contained in Reference 3.1.

(3) Information concerning licensee control and accounting procedures or inventory differences for special nuclear source or by-product material.

(4) Any information already in the public domain, including commercial safeguards equipment specifications, catalogs, and equipment buying data.

(5) Portions of guard qualification and training plans that do not disclose facility safeguards features or response procedures.

(6) Original design sketches of the physical protection system as well as initial requests for bids and proposals concerning this system.

(7) Drawings that show the location of safety-related equipment, unless a drawing is specifically made, overlaid, or annotated for the physical protection of CPNPP, are not SGI.

(8) General Information concerning the state or local police forces, such as a total compliment, shift, size, etc., that is already in the public domain.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-6

6. **(U)** Part 2, Section 13.6, Security (Page 13.6-1): Provide design and performance requirements for physical protection systems that are outside the scope of the referenced US-APWR DC. Indicate reference to MHI Technical Report, UAP-SGI-80002, US-APWR - High Assurance Assessment Evaluation Report, and the specific sections of the MHI technical report that describes the design and performance requirements for physical protection systems (PA security access point, sally port and vehicle barrier systems location and configurations, road layout to reduce force of vehicle impact) that will be relied on to provide a high assurance of adequate protection.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT and maintain at all time such capabilities. The design of physical protection systems beyond the scope of the DC is required as a COL information item, No. COL 13.6(2). Title 10 CFR 52.80(a) requires the application to contain information for ITA and criteria necessary and sufficient to provide reasonable assurance that the facility has been constructed and will operate in conformity with the combined license, the provisions of the Act, and the Commission's rules and regulations. The descriptions of design and performance requirements establish the design basis for licensing, detailed of design, and criteria for verification by inspections, tests, and/or analyses. The descriptions for the designs and performance requirements for physical protection systems may conform to guidelines of Regulatory Guide 1.206 to meet the requirement of 10 CFR 52.80(a).

(U) Note: The information addressing specific details related to security features or providing security functions will be safeguards information (SGI) and should be marked and protected in accordance with 10 CFR 73.21. The applicant should portion mark text in the response to request for additional information (RAI) as appropriate to identify SGI (or Official-Use-Only Security-Related Information) that reveals the specific details of physical protection.

ANSWER:

See the response to Question 13.06.01-1. In addition, Appendix A of the High Assurance Evaluation Assessment has been referenced in FSAR Subsection 13.6.1.

Impact on R-COLA

See attached marked-up FSAR Revision 1 page 13.6-1.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-7

7. **(U)** Part 2, Section 13.6.1, Physical Security - Combined License (Page 13.6-1): Indicate that security plans are submitted as Part 8 of the COL application.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73. Title 10 CFR 52.6, Completeness and accuracy of information, requires information provided "shall be complete and accurate in all material respects." The indicating that Part 8 of the COL application contains security plans would clarifies that security plans are not in a separate licensing document, but is part of the COL application.

ANSWER:

The CPNPP Units 3 and 4 COL Application, Part 8, contains the Physical Security Plan, the Security Training and Qualification Plan, and the Safeguards Contingency Plan, (collectively, "The Security Plan"). FSAR Section 13.6 has been revised to state that these plans are included in Part 8 and submitted with the application.

Impact on R-COLA

See attached marked-up FSAR Revision 1 page 13.6-1.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP`RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-8

8. **(U)** Part 2, Section 13.6,1, Physical Security - Combined License, Section 13.6.2.1, Barriers, Isolation Zones, and Controlled Access Point (Pages 13.6-1 to 13.6-2): Indicate reference to MHI Technical Report UAP-SGI-08002, US-APWR - High Assurance Assessment Evaluation Report, for meeting COL Information Items 13.6(2) and 13.6(5).

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73. Title 10 CFR 52.80(a) required the application to contain information for ITA and criteria necessary and sufficient to provide reasonable assurance that the facility has been constructed and will operate in conformity with the combined license, the provisions of the Act, and the Commission's rules and regulations. Applicant may conform to guidance of RG 1.206 in providing required descriptions of detailed design and performance requirements addressing COL Information Items No. 13.6(2) and No. 13.6(5).

(U) COL Information Item No. 13.6(2) states that. "[t]he COL applicant is to develop and provide as part of its physical security plan site specific physical security features and capabilities, such as (i) the physical barrier surrounding the protected area boundary; (ii) the isolation zone in areas adjacent to the protected area boundary, (iii) security lighting, or use of low-light technology, for the isolation zone and protected area; (iv) the vehicle barrier system, (v) controlled access points to control entry of personnel, vehicles and materials into the protected area, (vi) the intrusion detection system, and (vii) the closed circuit television camera and video assessment systems to provide monitoring and assessment of the protected area perimeter." COL Information item No. 13.6(5) states that "[t]he COL applicant's physical security plan is to make provision for radio or microwave transmitted two-way voice communication to communicate with the local law enforcement agencies." The design, performance requirements, and design basis for physical protection systems between the vital barriers and the PA and OCA are described in MHI Technical Report UAP-SGI-08002. Reference 13.06-201, security plans submitted under Part 8 of the COLA, contains limited descriptions for design and performance requirements for meeting regulatory requirements of 10 CFR 52.80(a).

ANSWER:

See the response to Question 13.06.01-1 above. CPNPP was the reference plant for the US-APWR assessments and, as such, the specific physical security features and capabilities of CPNPP are described in the US-APWR reports.

Impact on R-COLA

See attached marked-up FSAR Revision 1 pages 13.6-2 and 13.6-4 (SRI).

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-9

9. **(U)** Part 2, Section 13.6,2.2, Vital Area and Vital Equipment (Page 13.6-2): Describe the design and performance requirements for the interfaces between the central alarm station (CAS) and secondary alarm station (SAS) to address redundancies of functions (i.e., detection, assessments, and communications capabilities) based on the stated change to the DCD subsection 13.6.2.2. Specifically, provide the conceptual design descriptions and performance requirements for alarm system, configurations, and interfaces required to provide redundancies of capabilities for intrusion detection, assessment, and communications to and from the CAS and SAS, along with the design requirements for system interfaces between the CAS and SAS.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73. Title 10 CFR 73.55(i)(4)(G)(iii) requires that both alarm stations shall be equal and redundant. Title 10 CFR 52.80(a) requires that the application contain information for ITA and criteria necessary and sufficient to provide reasonable assurance that the facility has been constructed and will operate in conformity with the combined license. The MHI Technical Report UAP-SGI-08002 should be referenced as applicable for the site specific configurations for CAS and SAS.

(U) Note: The information addressing specific details related to security features or providing security functions will be safeguards information (SGI) and should be marked and protected in accordance with 10 CFR 73.21. The applicant should portion mark text in the response to request for additional information (RAI) as appropriate to identify SGI (or Official-Use-Only Security-Related Information) that reveals the specific details of physical protection.

ANSWER:

The Central Alarm Station (CAS) located in Unit 3 and the Secondary Alarm Station (SAS) located in Unit 4 are separate command and control centers located in robust structures. Each alarm station has complete and separate capabilities to support detection, alarm assessment, access control, communications, and response dispatch, command and control.

Both alarm stations are designed to be in full compliance with 10 CFR 73.55. Both alarm stations are protected as Vital Areas with all the associated protection elements required of Vital Areas. Both the CAS and SAS will be bullet-resisting in accordance with the requirements of 10 CFR 52. In accordance with the design basis threat of radiological sabotage defined in 10 CFR 73.1(a)(1), both alarm stations are designed and equipped to ensure that a single act cannot disable both alarm stations. Both alarm stations are configured such that their interiors are not visible from the perimeter of the protected area.

Both alarm stations are equal and redundant, such that all functions needed to address redundancies of functions (e.g., detection, assessments, and communications capabilities) can be performed in both alarm stations. Both alarm stations are supported by primary and back-up power systems. As depicted in Figure 1 below, each alarm station will have full capabilities to independently:

- receive alarms
- assess alarms with video monitors and video capture equipment
- administer access control functions
- communicate with security officers via radio, telephone, alternate telephone, and intercom
- communicate with offsite response forces via radio and telephone
- communicate with the Control Room
- control active barrier systems
- control security lighting used to support CCTV and visual assessment
- provide information and instructions via the plant notification system

Impact on R-COLA

None.

Impact on S-COLA

None.

Impact on DCD

None.

Central and Secondary Alarm Functionality and Redundancy

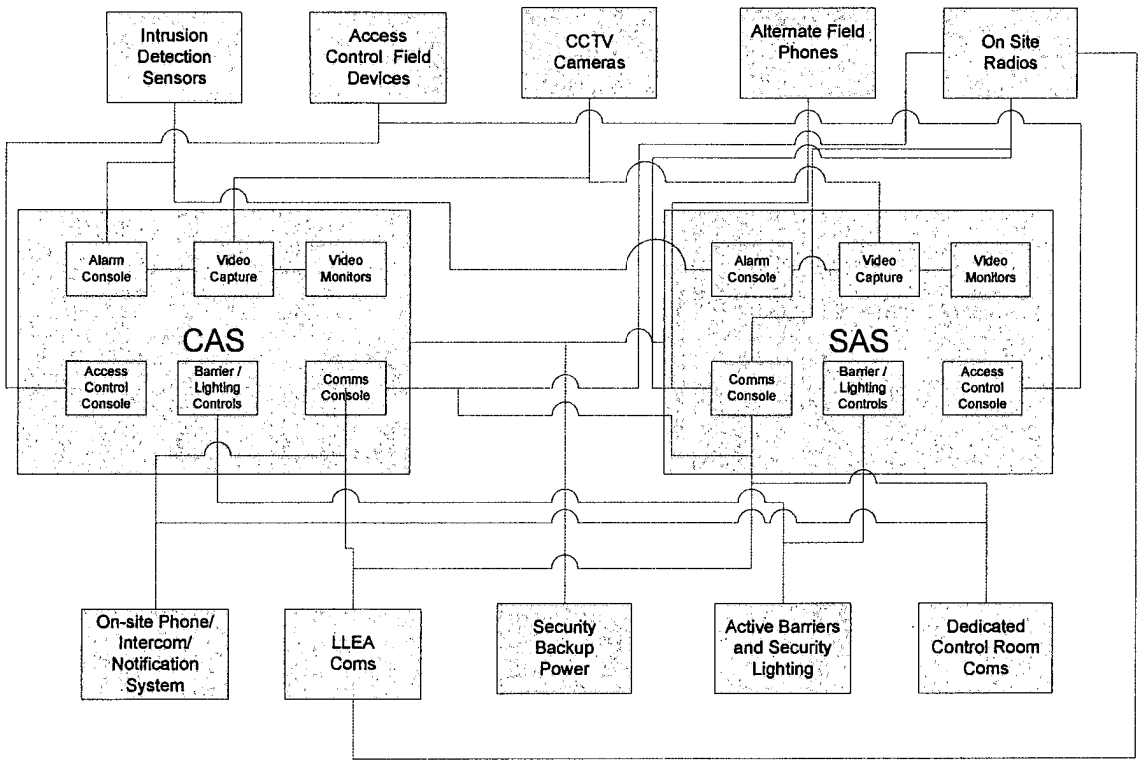


Figure 1
Conceptual Configuration of CAS and SAS Systems
(*Monitoring and control functions may reside in integrated consoles*)

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-10

10. **(U)** Part 2, Section 13.6,2.3, Alarm Systems and Detection Aids (Page 13.6-3): Provide descriptions of design and performance requirements for physical protection systems meeting regulatory requirements of 10 CFR 73.55(e)(7)(i)(c), for monitoring with assessment equipment that is designed to satisfy the requirements of § 73.55(i), and provide real-time and play-back/recorded video images of the assess activities before and after each alarm annunciation

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73. MHI Technical Report UAP-SGI-08002, U.S. APWR - High Assurance Assessment Evaluation should be incorporated by reference, if the descriptions of design and performance are applicable to the site specific configurations and physical protection that will be provided to detect and assess intrusions.

(U) Note: The information addressing specific details related to security features or providing security functions will be safeguards information (SGI) and should be marked and protected in accordance with 10 CFR 73.21. The applicant should portion mark text in the response to request for additional information (RAI) as appropriate to identify SGI (or Official-Use-Only Security-Related Information) that reveals the specific details of physical protection.

ANSWER:

CPNPP Units 3 and 4 employ CCTV, including video capture systems that are fully integrated with the alarm system for the complete detection and assessment of the PA and isolation zones by security force personnel that would respond to adversaries. The design and performance requirements for the monitoring with assessment equipment and real-time and play-back/recorded video images equipment are provided in Section 15.2 of the PSP and the High Assurance Evaluation Assessment, Appendix A. FSAR Subsection 13.6.2.3 has been revised to include reference to the PSP and the HAE.

Also, see the response to Question 13.06.01-1 above.

Impact on R-COLA

See attached marked-up FSAR Revision 1 page 13.6-3 (SRI).

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-11

11. **(U)** Part 2, Section 13.6,2.4, Security Lighting, Section 13.6.2.5, Security Communications Systems, and Section 13.6.2.6, Security Power (Pages 13.6-3 and 13.6.4): Indicate reference to MHI Technical Report UAP-SGI-08002, US-APWR - High Assurance Assessment Evaluation Report, that contains descriptions of design and performance requirements for security lighting.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73. Security systems design, performance requirements, and design basis for physical protection systems between the vital barriers and the PA and OCA are described in MHI Technical Report UAP-SGI-08002. The descriptions of design and performance requirements establish the design and basis for licensing and detailed design, which will be verified through ITA. The applicant may incorporated by reference the MHI technical report to establish the applicant's COL design and licensing basis and site specific requirements for meeting 10 CFR 52.80(a) requirements that the application contain information for ITA and criteria necessary and sufficient to provide reasonable assurance that the facility has been constructed and will operate in conformity with the combined license, the provisions of the Act, and the Commission's rules and regulations. The reference 13.06-201, security plans submitted under Part 8 of the COLA, contains limited descriptions for design meeting regulatory requirements of 10 CFR 52.80(a).

ANSWER:

See the response to Question 13.06.01-1. FSAR Subsection 13.6.2.4 has been revised to reference the PSP and High Assurance Evaluation Assessment, Appendix A.

Impact on R-COLA

See attached marked-up FSAR Revision 1 page 13.6-4 (SRI).

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-12

12. **(U)** Part 2, Section 13.6.4, Combined License Information (Page 13.6.4): Provide the following related to COL information items: (a) indicate the appropriate sections or parts of the COL application that describe the implementation schedule stated in the COL Information item 13.6(1); (b) indicate MHI Technical Report UAP-SGI-08002, in addition to Part 8, "physical security plan," for the descriptions of site specific physical protection systems design and performance requirements meeting for COL information item 13.6(2); and (c) include reference to MHI Technical Report UAP-SGI-08002 for meeting COL information item 13.6(5).

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73. Title 10 CFR 52.6, Completeness and accuracy of information, requires information provided "shall be complete and accurate in all material respects." MHI Technical Report UAP-SGI-80002 contains descriptions of design and performance requirements for physical protection systems that are within the scope of the COL applicant that should be incorporated by reference.

ANSWER:

(a) Table 13.4-201 and Part 10 of the COL Application, Section 3 outline a series of programmatic implementations related to specific milestones. Included in this listing are the Physical Security Plan, the Training and Qualifications Plan, and the Safeguards Contingency Plan, which are tied to the receipt of fuel on-site for CPNPP Units 3 and 4 (in the protected area). FSAR Subsection 13.6.4 has been revised to refer to Table 13.4-201 and Part 10, Section 3.

(b)(c) COL Information Items 13.6(2) and 13.6(5) in FSAR Subsection 13.6.4 have been revised to delete reference to the Physical Security Plan because the other sections listed already reference the Physical Security Plan and the High Assurance Evaluation Assessment.

Impact on R-COLA

See attached marked-up FSAR Revision 1 pages 13.6-4 and 13.6-5.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-13

13. **(U)** Part 2, Section 13.6,5, References (Page 13.6-4): Include, the MHI Technical Report UAP-SGI-08002, US-APWR - High Assurance Assessment Evaluation Report, as a reference.

(U) Regulatory Basis: The design of physical protection systems beyond the scope of the DC is required as COL Information Item 13.6.1. Title 10 CFR 52.6, Completeness and accuracy of information, requires information provided "shall be complete and accurate in all material respects." Title 10 CFR 52.80(a) required the application to contain information for ITA and criteria necessary and sufficient to provide reasonable assurance that the facility has been constructed and will operate in conformity with the combined license, the provisions of the Act, and the Commission's rules and regulations. Title 10 CFR 52.6, Completeness and accuracy of information, requires information provided "shall be complete and accurate in all material respects." The MHI Technical Report UAP-SGI-08002 contains details of design and licensing basis information for proposed nuclear operations.

ANSWER:

The HAE is incorporated by reference into the FSAR as part of DCD Section 13.6. Therefore, it does not need to be added to FSAR Subsection 13.6.5, References.

Impact on R-COLA

None.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-14

14. **(U)** General Comment (all portions of the security plans): Revise security plans to indicate consistently the name of the applicant (i.e., Luminant Generation Company LLC or Luminant, on behalf of Comanche Peak Nuclear Power Company LLC (CPNPC)) and the name of the generating plants (i.e., Comanche Peak Nuclear Power Plant Unit 3 and Unit 4, CPNPP Units 3 & 4, or CPNPP 3 and 4)).

(U) Regulatory Basis: Title 10 CFR 52.6, Completeness and accuracy of information, requires information provided "shall be complete and accurate in all material respects." The security plans uses the term "CPNPP" to identify the licensee and the plant, along with "CPNPP Unit 3 and 4" Part 1, Administration and Financial Information, Section 1.1, License Actions Requested, identifies Luminant and CPNPP as the recipients of the COL license for the new plant identified as "CPNPP Units 3 and 4" or CPNPP 3 & 4. These appear as a separate and distinct entity from the existing Comanche Peak nuclear power plant and must be accurate and consistently identified throughout the licensing document. The use of "CPNPP" is not consistent with Part 1 of the COL application, and it appears to refer to either the operating licensee or the new plants.

ANSWER:

The PSP will be reviewed and corrected to the names listed below to ensure consistency with the COLA. The correct references are:

- *Luminant Generation Company LLC (Luminant), who is the licensee for construction and operation of the new units,*
- *Comanche Peak Nuclear Power Company LLC (CPNPC), who is the licensee to own the new units, and*
- *Comanche Peak Nuclear Power Plant Units 3 and 4 (CPNPP 3 and 4) which is the name of the new units.*

Impact on R-COLA

The PSP will be revised to consistently use the terms of the licensee for construction and operation of the new units and the name of the new units as stated above.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-15

15. **(U)** Part 8, Physical Security Plan, Section 1.0, Introduction (Page 1): Indicate reference to regulatory requirements set forth in 10 CFR 52,79(a)(35)i, 52.79(a)(36)(i) and (ii) in lieu of "10 CFR 50.34(c) and (d)," for the COL application.

(U) Regulatory Basis: Title 10 CFR 52.6, Completeness and accuracy of information, requires information provided "shall be complete and accurate in all material respects." Subpart C of 10 CFR 52 establishes the regulatory requirements for CPNPP Units 3 and 4 combined license application. The security plans must meet requirements of 10 CFR 52 and the reference to the requirements of 10 CFR 50 as stated is not accurate.

ANSWER:

The referenced regulatory requirements, which are part of the black letter text in NEI 03-12, Revision 6, are the applicable regulatory requirements for operating plants licensed under 10 CFR 50, whereas 10 CFR 52,79(a)(35)(i), (36)(i), and (36)(ii) are the applicable regulatory requirements for plants licensed under 10 CFR 52. *Accordingly, the first paragraph of the Physical Security Plan, Section 1 will be revised to replace 10 CFR 50.34(c) and (d) with 10 CFR 52,79(a)(35)(i), (36)(i), and (36)(ii). The revised sentence will read as follows: "This document, including appendices, satisfies the regulatory requirements set forth in 10 CFR 52,79(a)(35)i, (36)(i), (36)(ii), and 10 CFR Part 73 to provide a Physical Security Plan for the Comanche Peak Unit 3 and 4 Plant." This will be identified as a change to the black letter text in the template.*

Impact on R-COLA

The revision to the PSP described above will be completed in the next revision to the COL Application.

Impact on S-COLA

None

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-16

16. **(U)** Part 8, Physical Security Plan (PSP), Section 1.1, Facility Physical Layout (pages 1-2): Provide clarification on whether Part 2, FSAR, Chapter 2, Site Characteristics, (i.e., Sections 2.1, Geography and Demography, 2.1.1, Site Location and Descriptions, 2.1.2, Exclusion Area Authority and Control, and 2.2, Nearby Industrial, Transportation, and Military Facilities) is applicable in providing additional details of the descriptions and Figures 1, 2, and 3 in PSP Section 1.1 for the meeting regulatory requirement of 10 CFR 73, Appendix C, Section II (B)(3)(b), Physical Layout. Provide a statement that references Part 2, FSAR, Chapter 2, Site Characteristics, for describing the facilities to complete and supplement information contained in Section 1.1 of the PSP.

(U) Regulatory Basis: Title 10 CFR 73, Appendix C, Section II (B)(3)(b), Physical Layout, requires the safeguards contingency plan to "include a site map depicting the physical structures located on the site, including onsite independent spent fuel storage installations (if applicable), and a description of the structures depicted on the map. Plans must also include a descriptions and map of the site in relation to nearby towns, transportation routes (*e.g.*, rail, water, and roads), pipelines, airports, hazardous material facilities, and pertinent environmental features that may have an effect upon coordination of response activities. Descriptions and maps must indicate main and alternate entry routes for law enforcement or other offsite response and support agencies and the location for marshaling and coordinating response activities." Applicant may reference COL application Part 2, FSAR, Chapter 2, which already contains descriptions of site characteristics that would provide acceptable detailed descriptions and maps that supplement the information described in Section 1.1 of the PSP.

ANSWER:

FSAR Section 2.1 provides a detailed narrative regarding general geography of the region, specific geography of the immediate vicinity of CPNPP Units 3 and 4, demographics of the immediate vicinity, and other specific details of the regions and population centers. Section 2.2 provides a detailed narrative of nearby industrial, transportation, and military facilities.

The information contained in FSAR Sections 2.1 and 2.2 provides additional description for Section 1.1 of the PSP. ***The PSP will be revised to include a reference to FSAR Chapter 2, Sections 2.1 and 2.2.***

Impact on R-COLA

The PSP will be revised to include a reference to FSAR Sections 2.1 and 2.2 in the next revision of the COL Application.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-17

17. **(U)** Part 8, Physical Security Plan, Section 2, Performance Objectives (5th sentence, Page 2): State appropriately the reference to 10 CFR 73, or indicate all other specific parts of 10 CFR 73 that are required for the design of a physical protection systems and programs for CPNPP Units 3 and 4 in the 5th sentence of the paragraph.

(U) Regulatory Basis: Title 10 CFR 52.6, Completeness and accuracy of information, requires information provided "shall be complete and accurate in all material respects." Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73. The performance and prescriptive requirements for physical protection of power reactors are described in various sections of 10 CFR 73, in addition to requirements stated in 10 CFR 73.55. The statement that "The physical protection system and programs described here in are designed to protect against the Design Basis Threat (DBT) of radiological sabotage in accordance with the specific requirements of 10 CFR 73.55 (a) through (r) or equivalent measures that meets the same high assurance objectives provided by paragraph (a) through (r)," did not include regulatory reference for descriptions in the security plan for meeting 10 CFR 73.56 (access authorization described in Section 14.1), 10 CFR 26 (fitness for duty described in Section 14.1), 10 CFR 73.58 (safety/security interface requirements - not described or discussed), 10 CFR 73.54 (digital systems security described in Section 23).

ANSWER:

The text in PSP Section 2 that provides the commitment to adopt 10 CFR 73.55 is black letter text in the NEI 03-12 template that is generically applicable to all plants using the template. Black letter text is verbatim language from the NRC-endorsed NEI 03-12, Revision 6 template. There are no site-specific conditions that would make this black letter text inapplicable to CPNPP Units 3 and 4 and therefore the NRC endorsed text remains unchanged for CPNPP Units 3 and 4.

Furthermore, 10 CFR 73.55(b)(7) and (b)(8) require a security program to establish, maintain, and implement, respectively, an access authorization program in accordance with 10 CFR 73.56 and a cyber security program in accordance with 10 CFR 73.56. Additionally, other provisions of 10 CFR 73.55, e.g., 10 CFR 73.55(b)(9)(ii)(B), 10 CFR 73.55(g)(7)(i) and (ii), require implementation of the applicable portions of 10 CFR 26, Hence, these provisions are captured by the general reference to 10 CFR 73.55 in PSP Section 2. The PSP does not address the 10 CFR 73.58 safety/security interface; therefore there is no need for Section 2 to include a reference to 10 CFR 73.58. As responded to in Question 13.06.01-18, the FSAR has been revised to address the safety/security interface as required by 10 CFR 73.58.

Luminant also understands that the NRC and NEI are currently discussing revisions to be made to the NEI template which would be issued as Revision 7. CPNPP programs are revised to address updates to NRC-endorsed templates as appropriate.

Impact on R-COLA

None.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-18

18. **(U)** General Comment, Part 8, Physical Security Plan, Section 2, Performance Objectives (Page 2), and Section 17, Review, Evaluation and Audit of the Physical Security Program (Page 28): Describe how the requirements of 10 CFR 73.58 for managing safety/security interface will be met. Provide descriptions in the FSAR (i.e., Part 2) that describe of how plant management controls and process will be applied to meet 10 CFR 73.58 to manage the safety/security for the CPNPP Units 3 and 4.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73. Title 10 CFR 52.6, Completeness and accuracy of information, requires information provided "shall be complete and accurate in all material respects." Title 10 CFR 73.58 states that each licensee shall assess and manage the potential for adverse effects on safety and security, including the site emergency plan, before implementing changes to plant configurations, facility conditions, or security. The application did not include descriptions, in any parts of the application, on how plant management controls and processes will address the management of safety/security interface to meet requirements of 10 CFR 73.58. The applicant's description for the management of safety/security interface indicated in Part 8, Section 17, Review, Evaluation and Audit of the Physical Security Program, did not adequately address how applicant will manage and plan to implement safety/security interface in accordance with regulatory requirements. Section 17 only addressed reviews and audits of program no longer than 12 months after changes. The descriptions of how the applicant will apply plant's management controls and processes to provide assurance that safety/security interface will be adequately managed should not be described in Part 8, security plans. Security plan should reference the requirements in described in the FSAR for completeness.

ANSWER:

The Comanche Peak Nuclear Power Plant has an existing plant procedure (STA-919, CPNPP Safety-Security Interface Requirements), which applies to CPNPP Units 1 and 2. STA-919 outlines the process for reviews of design changes and all safety/security interface issues, and accomplishing the objectives of

10 CFR 73.58. Under the procedure, the Operations Review Committee (ORC) and the Station Operations Review Committee (SORC), as well as other discipline representatives, have specific roles managing safety/security interface issues. FSAR Subsection 13.1.1.2.1 has been revised to describe the safety/security interfaces for CPNPP Units 3 and 4. STA-919 is attached as a typical example of how this program will be implemented for Units 3 and 4.

Attachment

STA-919, "Safety Security Interface Requirements"

Impact on R-COLA

See attached marked-up FSAR Revision 1 pages 13.1-3 and 13.1-4.

Impact on S-COLA

None.

Impact on DCD

None.

COMANCHE PEAK NUCLEAR POWER PLANT

STATION ADMINISTRATION MANUAL

ELECTRONIC CONTROLLED COPY

CHANGES ARE NOT INDICATED

LATEST CHANGE NOTICE EFFECTIVE DATE PCN-0002 / 03/31/10 12:00

Verify current status in the Document Control Database prior to use.

QUALITY RELATED

CPNPP SAFETY-SECURITY INTERFACE REQUIREMENTS

PROCEDURE NO. STA-919

REVISION NO. 0

SORC MEETING NO.: 10-003 DATE: 2/11/2010

EFFECTIVE DATE: 3/31/2010 1200

PREPARED BY (Print): David Keating Ext: 5556

TECHNICAL REVIEW BY (Print): Neil Harris Ext: 5449

APPROVED BY: Dave Kross Date: 3/25/2010

PLANT MANAGER

TABLE OF CONTENTS

SECTION	DESCRIPTION	PAGE
1.0	PURPOSE	3
2.0	APPLICABILITY	3
3.0	REFERENCES	3
4.0	DEFINITIONS/ACRONYMS	4
5.0	RESPONSIBILITIES	6
6.0	INSTRUCTIONS	10
6.1	Safety-Security Interface - General Overview	10
6.2	Screening Processes	13
6.3	Security Review and Evaluation	15
7.0	FIGURES	17
8.0	ATTACHMENTS/FORMS	17
	Attachment 8.A, "Examples of Planned and Emergent Activities and Conditions Potentially Impacting The Physical Protection Program"	18
	Attachment 8.B, "Safety-Security Interface Performance References"	19
	Attachment 8.C, "CPNPP Processes and Controls for Safety-Security Interface"	24
	Attachment 8.D, "Safety-Security Impact Review and Evaluation Flow Chart"	26
	Attachment 8.E, "Screening Process Criteria"	27
9.0	RECORDS	17

1.0 PURPOSE

1.1 The purpose of this procedure is to provide Comanche Peak Nuclear Power Plant (CPNPP) management controls and processes used to establish and maintain an effective interface between plant operational safety and security in accordance with 10 CFR 73.58 requirements. These controls and processes ensure that potential adverse impacts to plant operational safety and security are considered and addressed prior to implementation of a change to physical layout, facilities, structures, systems, components, and operating procedures. These controls and processes also address the safety and security impact of emergent plant conditions.

1.2 The following attachments do not require SORC review when being modified and issued per STA-202:
- Attachment 8.A, "Examples of Planned and Emergent Activities and Conditions Potentially Impacting The Physical Protection Program"
- Attachment 8.B, "Safety-Security Interface Performance References"
- Attachment 8.C, "CPNPP Processes and Controls for Safety-Security Interface"
- Attachment 8.D, "Safety-Security Impact Review and Evaluation Flow Chart"

2.0 APPLICABILITY

NOTE: CPNPP may expand or take credit for other plant processes to ensure an adequate interface between plant operational safety and security as indicated in this procedure.

2.1 This procedure applies to all planned and emergent activities and conditions that could compete/conflict with the CPNPP physical protection program as identified in Attachment 8.A, "Examples of Planned and Emergent Activities and Conditions Potentially Impacting The Physical Protection Program".

2.2 Reviews and audits of site physical protection program involving the safety-security interface.

3.0 REFERENCES

3.1 Performance References

- Refer to Attachment 8.B, "Safety-Security Performance References".

3.2 Developmental References

- Technical Specifications Section 5.0
- 10 CFR 73.58, "Safety-Security Interface Requirements for Nuclear Power Reactors"
- NRC Regulatory Guide 5.74, "Managing The Safety-Security Interface"

4.0 DEFINITIONS/ACRONYMS

4.1 Adverse Impact - A change impacts a plant or security system/equipment such that performance of the existing system, structure or component will be degraded. Adverse impacts and effects have the potential to increase the likelihood of malfunctions, increase consequences and to create new accidents.

4.2 Applicability Determination - A process for determining if a proposed activity, or portions thereof, is controlled by other more specific regulations and can be excluded from review under 10CFR50.59.

4.3 Emergency Preparedness Reviews - The review of an activity for potential emergency response impact is to determine if compensatory measures are needed to implement the Emergency Plan.

4.4 Exclusion Zone - An area that is a bounding mapped perimeter around CPNPP and is used for establishing effluent release limits and enables the licensee to fulfill their obligations with respect to the requirements of 10 CFR Parts 20 and 100 radiological criteria.

4.5 Isolation Zone - Any area adjacent to a protected area (PA) perimeter barrier (such as a fence) of sufficient width to permit observation and assessment of activities on either side of the protected area barrier. Isolation zones are clear, uncluttered areas between barriers (such as between a nuisance fence and PA fence) and provided with sufficient illumination and monitoring to detect possible intrusion of the protected area perimeter barrier.

4.6 Operations Review - The review of an activity for potential operations impact to determine if compensatory measures are needed to maintain the capability to safely shut down the reactor.

4.7 Plant Operational Safety-Security Interface - Safety-Security interface controls and processes that have been established to ensure potential adverse impacts to plant safety and security are considered and addressed prior to implementation of a change to physical layout, facilities, structures, systems, components, and operating procedures. These controls and processes also address the safety and security impact of emergent plant conditions.

4.8 Protected Area (PA) - The site area located inside the plant"s double fenced line and to which access is controlled.

4.9 Protected Area Breach - Opening in a PA barrier greater than 96 square inches with the smallest dimension no greater than six inches in any one direction.

4.10 Site Protective Strategy - The plan developed by CPNPP that is used to implement the intended actions of the site in response to attempts to commit radiological sabotage. Consists of CPNPP ability to respond to the external security design basis threat (i.e., adversaries and adversary characteristics) by focusing on (1) the interactions between the Operations and Security departments in establishing priorities for protecting equipment, and (2) the strategies used to protect that equipment [considered safeguards information (SGI)]. This effort may be impacted by the failure or degradation of communication systems, security response times, security/operator/emergency preparedness response/evacuation paths, equipment and systems critical to achieving and maintaining safe shutdown, protective defensive positions, security early warning system, Protected or Vital Area intrusion detection systems, security Protected Areas barrier degradation, isolation zone assessment capability, or security delay barrier degradation.

4.11 SME - Subject Matter Expert

4.12 Target Set - Means the combination of equipment or operator actions, which if all are prevented from performing their intended safety function or prevented from being accomplished, would likely result in significant core damage (e.g., non-incipient, non-localized fuel melting, and/or core disruption) barring extraordinary action by plant operators. A target set with respect to spent fuel sabotage is draining the spent fuel pool leaving the spent fuel uncovered for a period of time, allowing spent fuel heat up and the associated potential for release of fission products.

4.13 Temporary Modification - The temporary and reversible changes to plant systems, components or structures needed for short durations, to support plant operation or outages. These changes typically involve intrusive or intimate contact with systems, structures or components which are considered operable and not covered by another process control.

4.14 Vital Area - Posted area within the Protected Area that houses safety-related equipment. Access to the Vital Areas requires a Key Card Badge with appropriate management authorization or a properly trained and badged escort.

4.15 Vital Area (VA) Breach - Opening in a Units VA barrier greater than 96 square inches with the smallest dimension no greater than six inches in any one direction, except where it can be shown that the opening CANNOT be used to introduce materials which could damage vital equipment. Openings less than 96 square inches that could be used to introduce materials that could damage vital equipment from outside the barrier are also considered VA breaches.

4.16 Emergent Activity and/or Condition - An activity and/or condition that occurs/has occurred unexpectedly, requiring prompt assessment and evaluation to determine impact on the site protective strategy.

5.0 RESPONSIBILITIES

5.1 Security Shift Supervisor (SSS) in conjunction with the Luminant Security Manager or his designee evaluates the impact of planned and emergent plant conditions or activities on effective implementation of the site protective strategy. Responsibilities include the following:

5.1.1 Communicating those conditions impacting the site protective strategy including compensatory and mitigative measures to security shift personnel.

5.1.2 Interfacing with the Operations Shift Manager on a shiftly basis to identify emergent plant conditions or activities that have potential to adversely impact plant safety or security.

5.1.3 Notifying the Operations Shift Manager immediately when a protected area (PA) intrusion detection system segment fails and when the failures have been repaired/corrected and returned to service and/or resolved to a safe condition.

5.1.4 Attending the Plan of the Day meeting and informing the Operations Shift Manager of PA failures or planned PA activities that require compensatory posting including current status of the PA failures.

5.1.5 Attending routine site work control meetings to identify and screen conditions or activities that have potential to adversely impact plant safety and security (see section 6.3.2). The SSS will communicate identified conditions and activities to plant and security management and assist in evaluating impact and identifying compensatory and/or mitigative measures.

5.2 Luminant Security Manager notifies the SSS of emergent conditions or activities that may impact critical plant equipment and/or the site protective strategy. This may be performed by a Security Supervisor, Nuclear as a designee of the Luminant Security Manager. Assists security and operations staff in evaluating the impact of these conditions or activities on effective implementation of the security protective strategy and identification of compensatory and/or mitigative measures. Also has responsibility for maintaining this procedure.

5.3 Operations Shift Manager/Operations Day Shift Manager notifies the SSS of emergent conditions or activities that may impact safety related plant equipment and/or the site protective strategy. Assists security management staff in evaluating the impact of these conditions or activities on effective implementation of the security protective strategy and identification of compensatory and/or mitigative measures.

5.4 Security Work Coordinator (Luminant Security Coordinators or Security Operations Supervisor) (SWC)
attends routine site work control meetings to identify and screen conditions or activities that have potential to adversely impact plant safety and security (see section 6.3.2). The SWCs will communicate identified conditions and activities to plant and security management and assist in evaluating impact and identifying compensatory and/or mitigative measures.

5.5 Work Control/Outage Manager has responsibility for screening plant work activities for potential impact to security, operations or emergency response including, but not limited to:

- Any activity that requires placing items through a Protected or Vital Area fence (e.g, cords, tools, rope, etc.)
- Keeping security controlled zones clear of obstructions (e.g., vehicles, equipment / materials) at all times.
- Any work performed on power supplies that could affect security computers, lighting, or other security systems. (e.g., motor control centers, UPS systems, lighting panels, electric panels, electric buses, etc.).
- Any activity which would create an opening into a Protected or Vital Area barrier beyond established security limits.
- Any activity which would remove, relocate or degrade security related equipment.
- Scaffolding erection
- Temporary lighting
- Safety barrier erection
- Large tool box or drum storage
- Q and non-Q material storage

5.6 Chemistry Manager has responsibility for screening plant work activities for potential impact to security, operations or emergency response including, but not limited to

- Erection of chemical safety barriers
- Chemical containers or drums placement
- Chemical material storage
- Special chemical contamination control measures, water movement plans and impact to other organizations

5.7 Radiation Protection Manager has responsibility for screening radiation protection activities for potential impacts to security, operations or emergency response including, but not limited to

- Changes in radiological postings and barriers
- Changes in radiological conditions in the plant, e.g., draining or refilling systems, lowering water level in tanks and sumps, radiography, etc.
- Radiation safety barriers
- Movement of radiation protection equipment

5.8 Manager, Nuclear Emergency Planning has responsibility for screening emergency preparedness for potential impact to security.

5.9 Manager, Training shares responsibility with Work Organizations/Work Groups for training station personnel on the applicable portions of this program.

5.10 Senior Plant Management establish and support an effective interface between safety and security to ensure planned and emergent conditions or activities are evaluated for potential adverse impact on plant safety and effective implementation of the site protective strategy.

5.10.1 Director, Site Engineering and Support - has overall responsibility for screening plant design changes and related activities that may impact critical plant equipment and/or the site protective strategy.

5.10.2 Director, Plant Support has overall responsibility for screening emergent conditions or activities that may impact critical plant equipment and/or the site protective strategy.

5.10.3 Director, Operations has overall responsibility for notifying Security when an unplanned operability assessment entry is made for equipment within the scope of the Security ***target set*** equipment, and reviewing security activities for impact on manual operator actions listed in the Emergency Operating Guidelines and Off-Normal Operating Procedures. Scope of this responsibility is normally delegated to the Operations Shift Manager/Operations Day Shift Manager.

5.10.4 Director, Maintenance has overall responsibility for screening maintenance activities that may impact critical plant equipment and/or the site protective strategy, including, but not limited to

- Mechanical and electrical maintenance activities
- I & C calibration and maintenance activities
- Housekeeping activities that pertain to maintenance activities
- Work order package preparation activities
- Preparation, review and approval of maintenance, calibration, Fire Protection and I&C surveillance and test procedure activities
- Storage and access control activities for test equipment used to interface/communicate with plant digital assets
- Radiation monitoring system setpoint/background change activities

5.10.5 Shaw Director, Engineering and Technical Services has overall responsibility for screening proposed modifications for potential impact on Security, Operations or Emergency Preparedness.

5.10.6 Shaw Director, Maintenance/Support is responsible for screening facility work activities for potential impact to security, operations or emergency response including, but not limited to

- Scaffolding
- Safety barriers
- Large tool boxes or drums
- Security-controlled laydown area, isolation or exclusion zone encroachment
- Trailers or temporary buildings
- Security fields of fire or impact on intrusion detection/delay

5.10.7 Director, Oversight and Regulatory Affairs has overall responsiblity for performing periodic independent oversight to assess compliance with applicable elements of the Safety-Security Interface Program.

6.0 INSTRUCTIONS

6.1 Safety-Security Interface - General Overview

NOTE:
- Attachment 8.C, "Processes and Controls for CPNPP Safety-Security Interface" identifies CPNPP plant processes and controlling procedures by department organization that have been established to ensure an adequate interface between plant operational safety and security.
- CPNPP may expand or take credit for other plant processes and programs to ensure an adequate interface between plant operational safety and security as indicated in this procedure.

STA-919 is associated with the implementation of the Site Security Plan. The intent of this procedure is to establish and maintain an effective interface between plant operational safety and security at CPNPP, ensuring that potential adverse effects from implementation of changes to safety and security measures are considered and addressed prior to implementation.

The interface between plant operational safety and security is an important element of both programs relative to ensuring public health and safety. Plant activities that could compete or conflict with the capability of the site physical protection program to provide high assurance of adequate protection and common defense and security should be assessed.

Conversely, changes in the site physical protection program could also adversely affect plant operations; safety-related structures, systems, and components; operator actions; or emergency responses necessary to prevent or mitigate postulated design-basis accidents and to protect public health and safety and the environment.

CPNPP uses management controls for reviewing, assessing, and managing plant activities or changes to provide continued assurance of adequate safety and security; however, 10 CFR 73.58 adds a requirement for CPNPP to assess and manage changes to these activities effectively.

6.1.1 Management Controls and Processes

A. CPNPP utilizes the following management controls and processes to identify and manage planned and emergent changes, activities, and conditions to address potential adverse impact on plant operational safety and security:

1) Plan of the Day Meeting attended by Operations, Maintenance, Work Management, Engineering, Radiation Protection, Industrial Safety, Emergency Preparedness, and Security.

2) Plant procedures and practices to evaluate the impact of conditions or actions on plant operational safety and security.

3) Engineering change process controls and procedures that require impact reviews/evaluations be performed by interfacing groups.

4) Target set review and development by Security, Engineering, Information Technology, and Operations.

6.1.1 A. 5) Security and Industrial Safety participation in the work planning and control process.

6) The procedure revision process including technical review and approval under the requirements of STA-202.

7) Routine Operator rounds and Industrial Safety in-plant walk-downs.

8) Routine Security patrols.

9) Station Operations Review Committee (SORC) impact review and approval requirements.

10) Operations Review Committee (ORC) Oversight.

11) Routine Security assessments performed by Nuclear Oversight.

12) Security and Industrial Safety participation in outage planning.

13) Outage Control Center (OCC) operations for major outages and emergent work.

14) Limiting Conditions of Operation (LCO) determination and reporting.

15) Corrective Action Program (CAP).

16) Cyber security monitoring.

6.1.2 Safety-Security Interface - Initial Assessment

A. Operations and Security personnel performing routine rounds identify and report station activities which could impact nuclear safety or security.

B. Established management controls are utilized to determine and identify potential impacts to plant operational safety or security (refer to Section 6.1.1).

C. Planned and emergent activities, including procedure changes, are screened using screening criteria (refer to Section 6.2) to determine if the activity could affect plant operational safety and/or security.

- IF the results of a screening indicate security could be affected, THEN the activity is reviewed by Security.
- IF the results of a screening indicate plant safety could be affected, THEN the activity is reviewed by Operations.
- IF the results of a screening indicate emergency response could be affected, THEN the activity is reviewed by Emergency Preparedness.

6.1.2 D. Department Managers are required to update and/or maintain procedures, instructions, or desktop guidelines to ensure continuing compliance with the roles and responsibilities as defined in this procedure. Attachment 8.B, "Safety-Security Performance References", identifies the lower-tier procedures, instructions and desktop guidelines that are to be updated and maintained current with the requirements of this procedure.

6.1.3 Review of Planned and Emergent Conditions and Activities

A. Personnel knowledgeable of the site physical protection program and protective strategy review the following planned and emergent conditions and activities per existing site procedures, including but not limited to:

1) Activities that could result in the loss of primary power to security systems.

2) Installation or removal of safety or security barriers that could adversely impact plant operational safety, security or emergency response.

3) Placement of trailers or heavy equipment that could obstruct detection or assessment functions or increase response time or security personnel.

4) Installation of chemical or hazardous material storage tanks adjacent to protected defensive position.

5) Planned fire protection manual operator actions that do not account for paths of travel through the security response team's fields of fire which could delay or prevent operator response and invalidate safety assumptions and credited operator actions.

6) Construction activities that remove or degrade physical barriers, thus allowing established access controls to be bypassed.

7) Installation of safety barriers or structures that could increase the response time lines of armed personnel, that interfere with protected defensive position and fields of fire, or that interfere with or prevent detection and assessment functions.

8) Changes to target set equipment that could effect its availability or operability and impact the effective implementation of the site protective strategy.

6.2 Screening Processes

NOTE:
- IMMEDIATE NOTIFICATION to the Security Shift Supervisor or Security Operations Supervisor is required, if an identified potential adverse impact on the functions and performance of the elements of the site physical protection program that could result in the inadvertent degradation of site protective strategy, is associated with an **emergent activity or condition**.
- The screening process described below is only required if the activity/condition **not previously reviewed** has the potential to impact site protective strategy. Attachment 8.D, "Safety-Security Impact Review and Evaluation Flow Chart", outlines the screening and impact evaluation processes.
- Attachment 8.E, "Safety-Security Interface Screening Criteria", provides a list of specific questions that should be considered when evaluating activities or conditions that could produce a plant operational and safety interface impact. The responses to the screening criteria on Attachment 8.E provide the basis for further review and evaluation by Security.

6.2.1 CPNPP uses established processes to screen planned and emergent activities and conditions to identify and resolve potential conflicts that could have an adverse impact on plant operational safety and/or security. The established processes include, but are not limited to

- Applicability Determination (STA-707, OWI-007)
- Approved procedures and process controls outside the scope of STA-707

6.2.2 Planned and emergent activities and conditions that could compete/conflict with the plant operational safety and security interface include, but are not limited to those activities and conditions identified in Attachment 8.A, "Examples of Planned and Emergent Activities and Conditions Potentially Impacting The Physical Protection Program".

6.2.3 When a planned or emergent activity/condition **not previously reviewed** has been identified and/or initiated with the potential to create an adverse impact on the site protective strategy, then Attachment 8.E, "Screening Process Criteria" should be reviewed to assist in determining the following;

A. Does the activity have the potential to create an adverse impact on the functions and performance of the elements of the site physical protection program that could result in the inadvertent degradation of site protective strategy?

OR

B. Does the condition have the potential to create an adverse impact on the functions and performance of the elements of the site physical protection program that could result in the inadvertent degradation of site protective strategy?

6.2.4 IF the answer to one or more of the questions in Attachment 8.E is "YES", THEN a potential adverse impact on the functions and performance of the elements of the site physical protection program that could result in inadvertent degradation of site protective strategy has been identified for the planned or emergent activity and/or condition. Perform the following, as applicable, when notifying Security:

> NOTE: Planned activities involving procedure changes only, that potentially impact the site protective strategy, DO NOT require a Condition Report to be initiated. Refer to step 6.2.4 C.

A. **Planned Activity and/or Condition**

For a planned activity and/or condition, initiate a Condition Report in accordance with STA-421, "Initiation of Condition Reports", assigning ownership of the Condition Report to Security for further review and evaluation as described in Section 6.3.

B. **Emergent Activity and/or Condition**

For an emergent activity and/or condition, IMMEDIATELY NOTIFY the Security Shift Supervisor or Security Operations Supervisor that a potential plant operational safety and security interface impact has been identified. Security will process the review and evaluation as described in Section 6.3.

> NOTE: Changes to procedures that contain a potential adverse impact to site protective strategy, SHALL be reviewed by Security using the applicable STA-202 form that has been submitted.

C. **Procedure Change**

For changes to procedures, specify Security as a review organization on Form STA-202-1 for revisions or STA-202-7 for PCNs, as applicable, for further review and evaluation as described in Section 6.3.

6.2.5 IF ALL the answers to the questions in Attachment 8.E are "NO", THEN no further action is required under the scope of STA-919.

6.3 Security Review and Evaluation

NOTE: For emergent conditions determined by Security to adversely impact the site protective strategy:

- Compensatory measures and/or mitigative actions should be expedited and implemented as soon as possible as determined by the Security Shift Supervisor or Security Operations Supervisor.
- Security can implement compensatory measures and/or mitigative actions as deemed necessary prior to formally processing the review and evaluation in accordance with SEC-200.
- Security will ensure a Condition Report is initiated.

6.3.1 Upon notification of a potential plant operational safety and security interface impact by way of a Condition Report, Form STA-202-1, Form STA-202-7 or immediate notification due to an emergent condition, Security personnel, knowledgeable of the site physical protection program and protective strategy, initiate a review and evaluation of the activity or condition that has been identified in accordance with SEC-200, "Safety-Security Interface Evaluation".

6.3.2 Security assumes ownership of a Condition Report that addresses a potential plant operational safety and security interface impact and is responsible for reviewing and evaluating an identified potential interface impact in accordance with SEC-200.

6.3.3 IF the review and evaluation per SEC-200 determines that an adverse impact on the functions and performance of the elements of the site physical protection program has been identified, THEN ,

A. Security ensures compensatory measures and/or mitigative actions for emergent conditions are/have been initiated.

NOTE: Compensatory measures and/or mitigative actions to be taken involving Safeguards information are documented and filed in accordance with Safeguards requirements.

B. With the exception of Safeguards information, Security documents the results of SEC-200 review and evaluation in the associated Condition Report or on Form STA-202-1, page 2 of 2, as applicable, identifying the compensatory measures and/or mitigative actions to be taken, or that have been taken for emergent conditions.

C. Security ensures that compensatory measures and/or mitigative actions that have been identified and initiated are implemented.

D. The Condition Report can be completed following implementation of required compensatory measures and/or mitigative actions.

6.3.4 IF the review and evaluation per SEC-200 determines that an adverse impact on the functions and performance of the elements of the site physical protection program does NOT exist, THEN ,

A. Security documents the results of SEC-200 review and evaluation in the associated Condition Report or on Form STA-202-1, page 2 of 2, as applicable, identifying that no further action is required.

B. The Condition Report can be completed by Security.

7.0 FIGURES

None

8.0 ATTACHMENTS/FORMS

8.1 Attachments

8.1.1 Attachment 8.A, "Examples of Planned and Emergent Activities and Conditions Potentially Impacting the Physical Protection Program"

8.1.2 Attachment 8.B, "Safety-Security Interface Performance References"

8.1.3 Attachment 8.C, "CPNPP Processes and Controls for Safety-Security Interface"

8.1.4 Attachment 8.D, "Safety-Security Impact Review and Evaluation Flow Chart"

8.1.5 Attachment 8.E, "Screening Process Criteria"

8.2 Forms

None

9.0 RECORDS

None

ATTACHMENT 8.A
PAGE 1 OF 1

EXAMPLES OF PLANNED AND EMERGENT ACTIVITIES AND CONDITIONS POTENTIALLY IMPACTING THE PHYSICAL PROTECTION PROGRAM

1.0 Examples of planned and emergent activities and conditions that could potentially compete/conflict with the physical protection program include but are not limited to the following;

- Plant configuration changes
- Facility condition changes
- Security changes
- Design Modifications,
- Temporary Modifications,
- Condition Report impact reviews,
- Outage planning,
- Work activities,
- Material storage and laydown,
- Excavations
- Procedural changes,
- Changes to operator actions or security assignments,
- Maintenance activities,
- Emergency preparedness or planning
- Access modification or restrictions,
- Changes to the security plan and its implementation.
- Unplanned LCOARs
- Systems Important to Safety Log (SISL) entries

ATTACHMENT 8.B
PAGE 1 OF 5

SAFETY-SECURITY INTERFACE PERFORMANCE REFERENCES

1.0 The following CPNPP procedures have been identified as being impacted by the Safety-Security Interface program requirements;

- ABN-202, "Loss of Non-Safeguards Ventilation Systems"
- ABN-203, "Control Room Ventilation System Malfunction"
- ABN-601, "Response to a 138/345 KV System Malfunction"
- ABN-602, "Response to a 6900/480v System Malfunction"
- ABN-613, "25 KV Malfunction"
- ABN-905A, "Loss of Control Room Habitability"
- ABN-905B, "Loss of Control Room Habitability"
- ABN-907, "Acts of Nature"
- ALM-0022A, "Alarm Procedure 1-ALB-2B"
- ALM-0022B, "Alarm Procedure 2-ALB-2B"
- ALM-0064A, "Alarm Procedure 1-ALB-6D"
- ALM-0064A, "Alarm Procedure 2-ALB-6D"
- CHM-101, "Chemistry Administrative Control"
- CHM-116, "Chemistry Control of Temporary Chemical Injection/Feed Systems and Temporary Inline Instrumentation"
- CMP-SF-708, "Site Facilities Work Requests"
- ECE-1.03, "Preparation and Control of Engineering Administrative Procedures"
- ECE-1.03-01, "Preparation and Control of Engineering Technical Procedures"
- ECE-5.01, "Design Control Program"
- EOP-0.0A, "Reactor Trip or Safety Injection"
- EOP-0.0B, "Reactor Trip or Safety Injection"
- EPP-100, "Maintaining Emergency Preparedness"

ATTACHMENT 8.B
PAGE 2 OF 5

SAFETY-SECURITY INTERFACE PERFORMANCE REFERENCES

1.0 Performance References, continued

- ICA-101, "I&C Work Control"
- INC-3020, "Maintenance and Rework of Plant Doors"
- MDA-104, "Minor Work"
- MSE-P0-1328, "Cathodic Protection Annual Survey"
- MSM-C0-7310, "Service Water Pump Maintenance"
- MSM-C0-8809, "Crosby Main Steam Safety Valve Maintenance"
- MSM-C0-9825, "Personnel Airlock Maintenance"
- MSM-C0-9826, "Emergency Escape Airlock Corrective Maintenance"
- MSM-C0-9827, "Equipment Hatch Corrective Maintenance"
- MSG-3000, "Plant Radio System Maintenance"
- ODA-102, "Conduct of Operations"
- ODA-203, "Preparation of Abnormal Conditions Procedures"
- ODA-204, "Preparation of Emergency"
- ODA-207, "Guidelines on the Preparation and Review of Operations Procedures"
- ODA-308, "LCO Tracking Program"
- OPERATIONS GUIDELINE 06, "Operations Management Overview Program"
- OPERATIONS GUIDELINE 11, "Local Actions for Plant Events"
- OPT-430A, "Train A Integrated Test Sequence"
- OPT-430B, "Train A Integrated Test Sequence"
- OPT-435B, "Train B Integrated Test Sequence"
- OPT-0464A, "TRAIN A SAFEGUARDS SLAVE RELAY K602 ACTUATION TEST"
- OPT-0464B, "TRAIN A SAFEGUARDS SLAVE RELAY K602 ACTUATION TEST"
- OPT-803A, "Appendix J Leak Rate Test of Emergency Airlock (CP1-MEMEPE-01)"

ATTACHMENT 8.B
PAGE 3 OF 5

SAFETY-SECURITY INTERFACE PERFORMANCE REFERENCES

1.0 Performance References, continued

- OPT-803B, "Appendix J Leak Rate Test of Emergency Airlock (CP2-MEMEPE-01)"
- OPT-804A, "Appendix J Leak Rate Test of Emergency Airlock Door Seals (CP1-MEMEPE-01)"
- OPT-804B, "Appendix J Leak Rate Test of Emergency Airlock Door Seals (CP2-MEMEPE-01)"
- OWI-007, "Operations Procedure Development and Process Control Review Summary"
- OWI-104, "Operations Department Logkeeping and Equipment Inspections"
- OWI-110, "Operations Work Control and Clearance and Safety Tagging"
- RPI-263, "RMC Activities"
- RPI-273, "Rad-Vault/Trailer Inspections and Movement"
- RPI-602, "Radiological Surveillance and Posting"
- RPI-624, "Resin Transfer Job Coverage"
- SEC-102, "Control of Security Plans, Procedures, Instructions and Forms"
- SEC-200, "Safety-Security Interface Evaluation"
- SOP-604A, "480 VAC Switchgear and MCCs"
- SOP-604B, "480 VAC Switchgear and MCCs"
- SOP-610A, "Diesel Generator Fuel Oil and Transfer System"
- SOP-610B, "Diesel Generator Fuel Oil and Transfer System"
- SOP-613A, "Outage Power"
- SOP-613B, "Outage Power"
- SOP-907A, "Containment Personnel Airlocks"
- SOP-907B, "Containment Personnel Airlocks"
- STA-109, "Conduct of Maintenance"
- STA-116, "Maintenance of CPNPP Licensing Basis Documents, Operating License Conditions, and Technical Specifications"

ATTACHMENT 8.B
PAGE 4 OF 5

SAFETY-SECURITY INTERFACE PERFORMANCE REFERENCES

1.0 Performance References, continued

- STA-117, "Non-Radiological Environmental Protection Program"
- STA-122, "Infrequently Performed Tests or Evolutions"
- STA-123, "Pre-Job and Post-Job Briefs"
- STA-152, "Request for Procurement of Services"
- STA-153, "Management of Contracts"
- STA-202, "Nuclear Generation Procedure Change Process"
- STA-308, "Protection of Safeguards Information and Safeguards Information-Modified"
- STA-401, "Station Operations Review Committee"
- STA-421, "Initiation of Condition Reports"
- STA-422, "Processing Condition Reports"
- STA-425, "Materials Control"
- STA-602, "Temporary Modifications and Transient Equipment Placements"
- STA-604, "Configuration Risk Management and Work Scheduling"
- STA-606, "Control of Maintenance and Work Activities"
- STA-620, "Containment Entry"
- STA-627, "Control of Planned Outages"
- STA-629, "Switchyard Control"
- STA-632, "Forced Outages"
- STA-637, "Barricades and Barriers"

ATTACHMENT 8.B
PAGE 5 OF 5

SAFETY-SECURITY INTERFACE PERFORMANCE REFERENCES

1.0 Performance References, continued

- STA-661, "Non-Plant Equipment Storage and Use Inside Seismic Category I Structures"
- STA-682, "Control of Station Diving Operations"
- STA-686, "Control of Radiography Operations at CPNPP"
- STA-690, "Erecting and Control of Scaffolding"
- STA-696, "Hazard Barrier Controls"
- STA-699, "Configuration Management Program"
- STA-707, "10 CFR 50.59 Reviews"
- STA-716, "Modification Process"
- STA-729, "Control of Transient Combustibles Ignition Sources and Fire Watches"
- STA-753, "Control of Site Excavation"
- STA-902, "Access to CPNPP Site Areas"
- STA-904, "Vehicle and Material Package Control"
- STA-919, "CPNPP Safety-Security Interface Requirements"
- TSP-709, "Processing PPT Procedures and Results"
- WCI-203, "Weekly Surveillances / Work Scheduling"
- WCI-606, "Work Control Process"
- WCI-627, "Planned Outage Control Process"

ATTACHMENT 8.C
PAGE 1 OF 2

CPNPP PROCESSES AND CONTROLS
FOR
SAFETY-SECURITY INTERFACE

CPNPP PROCESSES *(NOTE 1)*	CONTROL for SAFETY-SECURITY INTERFACE
Administration - Procedure Changes	- STA-707, "10 CFR 50.59 Reviews"
Operation Activities - Procedure Changes - Unplanned LCOARs/SISLs, SRO Review - Operations Department Responsibilities - Operations Log Routine Inspections - Emergent Work Review	- STA-707, "10 CFR 50.59 Reviews" - OWI-007, "Operations Procedure Development and Process Control Review Summary" - ODA-308, "LCO Tracking Program" - ODA-102, "Conduct of Operations" - OWI-104, "Operations Department Logkeeping and Equipment Inspections" - OWI-110, "Operations Work Control and Clearance and Safety Tagging"
Work Activities - Procedure Changes - Work Order Prep - Emergent Work - POD - Outage Work	- STA-707, "10 CFR 50.59 Reviews" - STA-604, "Configuration Risk Management and Work Scheduling" - STA-606, "Control of Maintenance and Work Activities" - STA-627, "Control of Planned Outages" - STA-632, "Forced Outages" - WCI-203, "Weekly Surveillances/Work Scheduling" - WCI-606, "Work Control Process" - WCI-627, "Planned Outage Control Process
RP Activities - Procedure Changes - Boundaries, Barricade - Material Storage	- STA-707, "10 CFR 50.59 Reviews" - STA-660, "Control of High Radiation Areas" - STA-652, "Radioactive Material Control" - RPI-602, "Radiological Surveillance and Posting"
Chemistry Activities - Procedure Changes - Boundaries, Barricades - Material Storage	- STA-707, "10 CFR 50.59 Reviews" - STA-637, "Barricades and Barriers" - STA-626, "Chemical/Consumable Control Program" - STA-729, "Control of Transient Combustibles Ignition Sources and Fire Watches"
Emergency Planning Activities - Procedure Changes	- STA-707, "10 CFR 50.59 Reviews"

ATTACHMENT 8.C
PAGE 2 OF 2

CPNPP PROCESSES AND CONTROLS
FOR
SAFETY-SECURITY INTERFACE

CPNPP PROCESSES *(NOTE 1)*	CONTROL for SAFETY-SECURITY INTERFACE
Engineering Activities - Procedure Changes - FDA preparation for Design Modifications - Temporary Modifications	- STA-707, "10 CFR 50.59 Reviews" - ECE-5.01-08, "Electronic Design Change Process" - STA-602, "Temporary Modifications and Transient Equipment Placements"
Maintenance Activities - Procedure Changes	- STA-707, "10 CFR 50.59 Reviews"
Security Activities - Compensatory and/or mitigative actions	- SEC-200, "Safety-Security Interface Review and Evaluation"

Notes:

1 Activities are considered previously reviewed when planned and implemented per the normal work control and scheduling processes. Normal work control and scheduling processes credit Security notification and awareness through Security's participation in the following at power and outage activities, such as

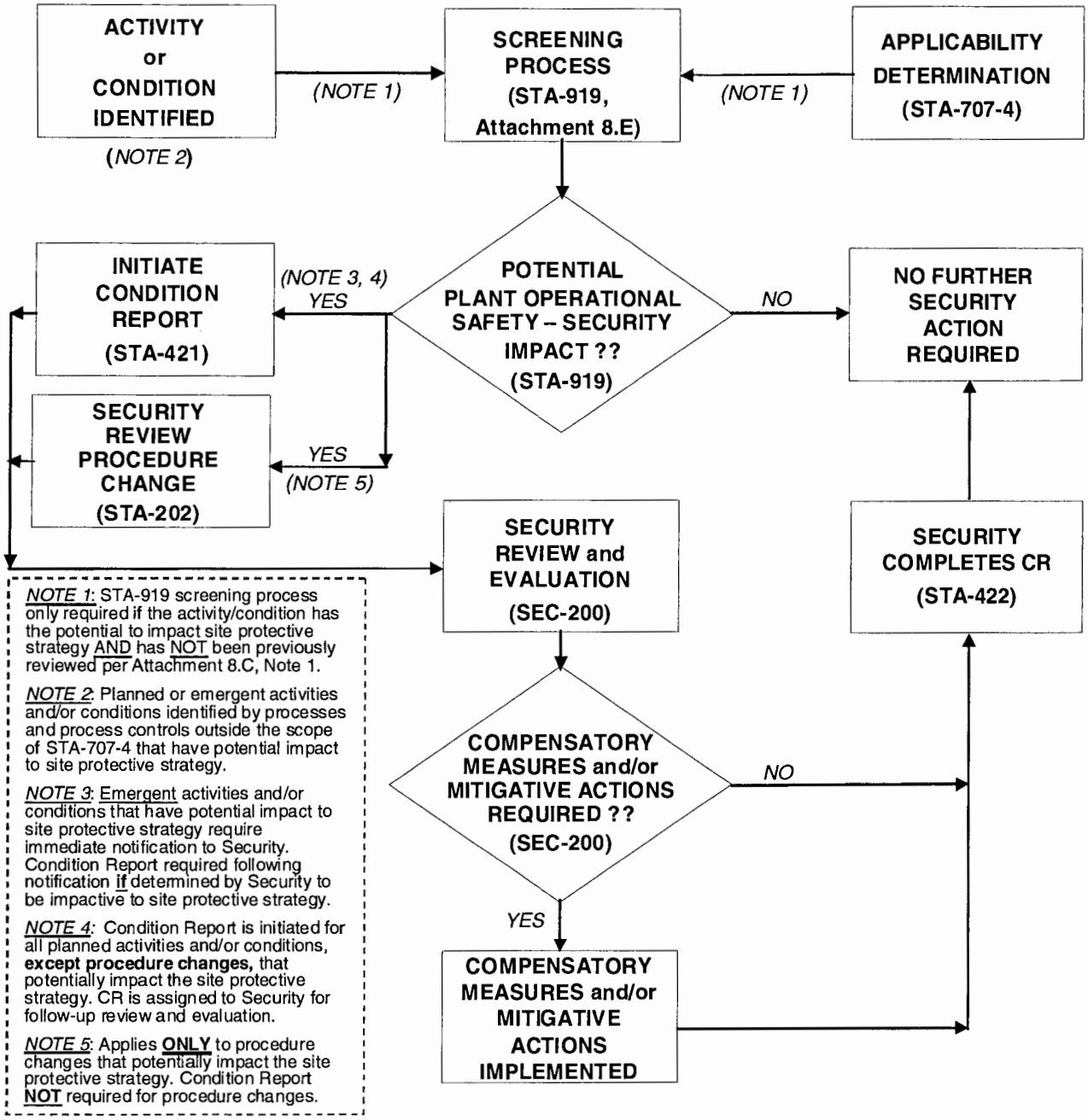
At Power
- Operational Decision Making (NMG-701)
- Plan of the Day (POD) meeting
- Schedule work week review (T-7, T-4 and T-2 schedule reviews)
- Shiftly Review of new Work Requests and activities
- Daily new Work Request and activity priority/scheduling reviews
- Work week package approval

Outage
- Forced Outage Recovery Planning meeting
- Outage Duty Manager notifications
- Outage Control Center (OCC) meetings
- Outage turnover meetings

Communication between work organizations and Security may suffice for assuring Safety-Security Interface requirements are met, depending on the complexity of the task(s) being performed and necessity for compensatory actions. For example, movement of heavy equipment, cranes, vehicles, etc. outside of pre-designated parking areas would normally only require verbal notification to Security of the intended movement.

ATTACHMENT 8.D
PAGE 1 OF 1

SAFETY-SECURITY IMPACT REVIEW
AND
EVALUATION FLOW CHART



NOTE 1: STA-919 screening process only required if the activity/condition has the potential to impact site protective strategy AND has NOT been previously reviewed per Attachment 8.C, Note 1.

NOTE 2: Planned or emergent activities and/or conditions identified by processes and process controls outside the scope of STA-707-4 that have potential impact to site protective strategy.

NOTE 3: Emergent activities and/or conditions that have potential impact to site protective strategy require immediate notification to Security. Condition Report required following notification **if** determined by Security to be impactive to site protective strategy.

NOTE 4: Condition Report is initiated for all planned activities and/or conditions, **except procedure changes,** that potentially impact the site protective strategy. CR is assigned to Security for follow-up review and evaluation.

NOTE 5: Applies **ONLY** to procedure changes that potentially impact the site protective strategy. Condition Report **NOT** required for procedure changes.

ATTACHMENT 8.E
PAGE 1 OF 3

SCREENING PROCESS CRITERIA

NOTE:
- The following pre-determined screening process criteria have been established to assist in identification and resolution of potential conflicts that could have an adverse impact on the functions and performance of the elements of the site physical protection program.
- IF the answer to one or more of the following questions is "YES", THEN a potential adverse impact on the functions and performance of the elements of the site physical protection program has been identified.
- IMMEDIATE NOTIFICATION to the Security Shift Supervisor or Security Operations Supervisor is required, if an identified potential adverse impact on the functions and performance of the elements of the site physical protection program that could result in the inadvertent degradation of site protective strategy, is associated with an **emergent activity and/or condition**.

1.0 INITIAL SCREENING

1.1 Planned and Emergent Activities or Conditions

A. The following criteria should be used to assist in determining potential plant operational safety and security impact associated with Planned and Emergent activities and/or conditions.

1) Does the proposed activity or condition affect the location within the plant, capacity (pump flow/head, tank volume, battery, etc.) or power source of:

a) Alternate and/or normal decay heat removal systems including high and low head primary and secondary makeup capability and containment post-accident heat removal?

b) Normal and/or remote safe shutdown instrumentation or controls including normal and alternate power capability?

c) Station Blackout capabilities, including electrical cross-ties?

d) Fixed or mobile fire suppression pump systems?

2) Does the proposed activity or condition have an impact on the location or use of any of the following:

- Physical barriers, walls or fences
- Isolation zones
- Personnel or vehicle access control points
- Detection, surveillance or communications equipment
- Plant exterior lighting or lighting levels
- Heavy equipment operation within the Protected Area

ATTACHMENT 8.E
PAGE 2 OF 3

SCREENING PROCESS CRITERIA

1.1 A. 3) Does the proposed activity or condition result in any excavation?

4) Does the proposed activity or condition affect the location, addition or deletion of any large, safety-related components?

5) Does the proposed activity or condition call out or name any security special features or locations, such as intrusion detection equipment, bullet resistant enclosures (BRE), duress controls, data gathering panels or access control panels?

6) Does the proposed activity or condition create a pathway through or under a Vital Area/Protected Area barrier (PA breach or VA breach)?

7) Does the proposed activity or condition provide any climbing aids adjacent to a Vital Area/Protected Area barrier?

8) Does the proposed activity or condition alter the structural integrity of a Vital Area/Protected Area barrier, including door hardware?

9) Does the proposed activity or condition alter any bullet-resisting barrier?

10) Does the proposed activity or condition alter the existing view of the Protected Area or isolation zone from a bullet resistant enclosure (BRE) position by placement of obstructions or changes in lighting?

11) Does the proposed activity or condition alter or affect the power supplies related to security computers, station UPS, intrusion detection equipment, lighting or any plant communications system?

12) Does the proposed activity or condition affect the plant communications system?

13) Does the proposed activity or condition add buildings, structures, or equipment where additional lighting is necessary to maintain minimum security lighting levels (to prevent hiding places)?

14) Does the proposed activity or condition affect a locked and alarmed or card-keyed security area?

15) Does the proposed activity or condition change the location of a Vital Area/Protected Area barrier?

16) Does the proposed activity or condition require placing items through a Protected or Vital Area fence (e.g, cords, tools, rope, etc.)?

ATTACHMENT 8.E
PAGE 3 OF 3

SCREENING PROCESS CRITERIA

1.1 A. 17) Does the proposed activity or condition require reaching or extending over a Protected or Vital Area fence or wall?

18) Does the proposed activity or condition require breaching a security barrier; e.g., portal, gate, manhole, vault plug, hatch, panel, fence, grating, etc.

19) Does the proposed activity or condition remove plant equipment and may cause security barrier breaches into areas/equipment such as circulating water pumps, service water pumps, MSIV, main feedwater valves, etc.

B. IF the answer to one or more of the above questions is "YES", THEN a potential adverse impact on the functions and performance of the elements of the site physical protection program that could result in inadvertent degradation of site protective strategy has been identified for the activity or condition. Perform the following;

- Proceed to Step 6.2.4 and complete the required action, as applicable, to notify Security.

C. IF ALL the answers to the above questions are "NO", THEN no further action is required under the scope of STA-919.

Record of Changes

Rev/PCN	Affected Pages	Description of Change
0 / 0	ALL	STA-919 is a new procedure, which provides Comanche Peak Nuclear Power Plant (CPNPP) management controls and processes used to establish and maintain an effective interface between plant operational safety and security in accordance with 10 CFR 73.58, "Safety/Security Interface Requirements for Nuclear Power Reactors" requirements. These controls and processes ensure that potential adverse impacts to plant operational safety and security are considered and addressed prior to implementation of a change to physical layout, facilities, structures, systems, components, and operating procedures. These controls and processes also address the safety and security impact of emergent plant conditions.

Rev/PCN	Affected Pages	Description of Change
0 / 1	5, 13, 14, 15, 16, 20, 22, 23, 26, 27, 29	PCN 1 incorporates the following changes as an administrative enhancement to improve the Safety-Security interface process and for clarification to improve reader understanding; 1. Definition 4.16: new definition added for clarification and source of consistency throughout procedure. "*Emergent activities and/or conditions*" is intended to mean all activities and/or conditions that have not been planned or scheduled. 2. NOTE prior to step 6.2.1, 1st bullet: replaced "...*existing condition*..." with "...*emergent activity and/or condition*..." for clarification to the end user and consistency throughout procedure. 3. Step 6.2.4: modified to provide clarification and consistency as described in item 1. and 2. above, and to provide enhanced direction to the end user on how a planned or emergent activity and/or condition should be processed for review by Security. a. 1st paragraph: inserted "...*planned or emergent* ..." prior to "*activity*..." for clarification and consistency. b. 6.2.4 A., 6.2.4 B. and NOTE: new steps added for Planned and Emergent activities and/or conditions, respectively for consistency with procedure content and due to different requirements to process these two distinct categories of activities and conditions, i.e. Planned and Emergent. Preceding NOTE is intended to emphasize that procedure changes needing Security review and evaluation, although planned, are to be processed under separate requirements as described in new step 6.2.4 C. c. 6.2.4 C. and NOTE: new step and NOTE for processing procedure changes that contain potential adverse impact(s) to the site protective strategy. Step is intended to take advantage of an existing administrative process (STA-202) for Security's review and evaluation, thus eliminating the need to generate a Condition Report. 4. NOTE prior to 6.3.1: changed "...existing conditions" to "...emergent conditions" for consistency and clarification; in 2nd bullet, deleted reference to STA-202 as SEC-200 already contains reference to STA-202 for procedure changes. Added 3rd bullet requiring Security to ensure that a Condition Report is issued. 5. Step 6.3.1: replaced "...*existing condition*..." with "...*emergent condition*..." for consistency and clarification. Also inserted "...*Form STA-202-1, Form STA-202-7* which are used to notify Security when a procedure change with a potential adverse condition is planned. 6. Step 6.3.3 A. and 6.3.3 B.: changed "...existing conditions" to "...emergent conditions" for consistency and clarification. In 6.3.3 A., deleted reference to Security Shift Supervisor or Shift Operations Supervisor as it is not an option (i.e. deemed necessary) to initiate compensatory actions when an adverse condition has been identified. 7. Step 6.3.3 B. and 6.3.4 A.; inserted "...*STA-202-1, page 2 of 2, as applicable*..." to account for how procedure reviews are documented by Security for the end users. 8. Attachment 8.B, pages 2,4 and 5 of 5: deleted MDA-101, STA-650/-652/-660 from list as these procedures have been determined by responsible departments to be not applicable. 9. Attachment 8.D: added new process box and Note 5 to flow chart to account for procedure reviews and evaluations using STA-202. 10. Attachment 8.D,Note 3 and Attachment 8.E. NOTE prior to step 1.0: replaced "...*existing condition*..." with "...*emergent activity and/or condition*..." for clarification to the end user and consistency throughout procedure. 11. Attachment 8.E, step 1.1 B: modified step by replacing action steps 1.1 B. 1)/2)/3) with a bulleted statement to proceed to and complete step 6.2.4, as applicable, to notify Security for the potential adverse impact identified.

Rev/PCN	Affected Pages	Description of Change
0 / 2	20, 22, 23, 24, 25, 26	PCN 2 incorporates the following changes: 1. Attachment 8.B: added MSM-C0-9825, MSM-C0-2826, OPT-435B, STA-117 and STA-919 to the Performance Reference list due to their applicability to the Safety-Security Interface process; deleted STA-119 and STA-429 due to their non-applicability to the Safety-Security Interface; also, editorially changed existing MSM-CO prefixes to MSM-C0 (zero) 2. Attachment 8.C: added new Note 1 to clarify and take credit for existing CPNPP processes that already incorporate a Safety-Security Interface (S-SI) for determining whether or not a potential activity and/or condition poses a potential adverse impact to the site protective strategy. Security is intimately involved in many of the existing work and planning process that occur daily and routinely (as identified in Note 1), providing Security the ability to promptly make a determination of any activity and/or condition's potential impact upon on the plant protective strategy without the need for the work group's to initiate a screen per Attachment 8.E. Security would still be required to ensure a Condition Report was initiated if any activity or condition identified during their participation and overview of the work and planning processes was determined to be a potential adverse impact on the site protective strategy. 3. Attachment 8.D, Note 1: modified Note, referencing new Attachment 8.C, Note 1 for continuity. Also deleted "*IF REQUIRED*" (two places) on flow chart. Note 1 already refers to "STA-919 screening process only required if ...." thereby eliminating redundancy.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-19

19. **(U)** Part 8, Physical Security Plan, Section 4, Establishment of Security Organization (Page 4): Clarify and indicate that the contract services, the security organization contractor, plans to meet and implement all remaining requirements of 10 CFR 73 applicable to a power reactor licensee, in addition to the requirements "10 CFR 73.55(b)(1)(i) through (iv) and (b)4(i)" indicated in Section 4.

(U) Regulatory Basis: Title 10 CFR 52.6, Completeness and accuracy of information, requires information provided "shall be complete and accurate in all material respects." The performance and prescriptive requirements for physical protection of power reactors are described in various sections of 10 CFR 73, in addition to requirements stated in 10 CFR 73.55. Clarification is needed to ensure that Luminant contracted service plans to meet and implement all applicable requirements of 10 CFR 73 and not only 10 CFR 73.55.

ANSWER:

Luminant is responsible for all requirements of 10 CFR 73 whether it employs a contractor or not. The last two sentences from the first paragraph of Section 4 on page 3-4 provide no value and will be deleted.

Impact on R-COLA

The PSP will be revised in the next revision of the COLA.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-20

20. **(U)** Part 8, Physical Security Plan, Section 4.1, Security Organization Management (Page 4): Delete "Update" in "Updated Final Safety Analysis Report" and delete "U" from "UFSAR."

(U) Regulatory Basis: Title 10 CFR 52.6, Completeness and accuracy of information, requires information provided "shall be complete and accurate in all material respects." The facility management organization is outlined in the Updated Final Safety Analysis Report, as titled in the COL application, Part 2. For the purpose the COL application, FSAR is the appropriate and accurate reference to Part 2 of the application. Update to FSAR is performed after licensing and would be identified as "UFSAR".

ANSWER:

The references to the Updated Final Safety Analysis Report and UFSAR, which are part of the black letter text in NEI 03-12, Revision 6, are applicable for plants that are currently licensed and operating, but not for plants currently undergoing licensing. *Accordingly, the PSP, Section 4.1, page 4 will be revised to replace the terms "Updated Final Safety Analysis Report", and "UFSAR", with "Final Safety Analysis Report" and "FSAR," respectively. The black text change list will be revised to add this change.*

Impact on R-COLA

The PSP will be revised in the next COLA revision.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-21

21. **(U)** Part 8, Physical Security Plan, Section 4.1, Security Organization Management (Page 5): Delete "proprietary" and "or other qualified personnel" in the 6th paragraph on Page 5 to provide consistency with the statement in the first paragraph of Page 4 (i.e., "[t]he Security Force at CPNPP is a contract service").

(U) Regulatory Basis: Title 10 CFR 52.6, Completeness and accuracy of information, requires information provided "shall be complete and accurate in all material respects." Luminant states that the security force for CPNPP Units 3 and 4 is a contract service.

ANSWER:

The last two sentences from the first paragraph of PSP Section 4 on pages 3 and 4 will be deleted (refer to the response to Question 13.06.01-19 above). As a result of that revision, no change is required to the 6th paragraph on Page 5 in Section 4.1.

Impact on R-COLA

None.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-22

22. **(U)** Part 8, Physical Security Plan, Section 4.1, Security Organization Management (Page 4): Delete "(Security Shift Supervisor qualified)" in the 5th paragraph of Section 4.1.

(U) Regulatory Basis: Title 10 CFR 52.6, Completeness and accuracy of information, requires information provided "shall be complete and accurate in all material respects." The qualification of Armed Response Team Leader (RTL) is addressed in the Table 1, Critical Tasks Matrix, of applicant Training and Qualification Plan. The Security Shift Supervisor (SSS), 2nd to last paragraph, states that the SSS does not have other routine assignments that would preclude their ability to direct all activities of the security organization. The quote implies that the SSS may also be a RTL, which would be contrary to regulatory requirement of 10 CFR 73.55(d)(2)(ii) that at least one member, on site and available at all times, who has the authority to direct the security activities and is assigned no other duties. Designation as a RTL interferes with this individual's ability to perform duties as a SSS.

ANSWER:

The 6th paragraph of PSP Section 4.1 will be revised to delete the phrase "(Security Shift Supervisor qualified)."

Impact on R-COLA

The PSP will be revised in the next COLA revision.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-23

23. **(U)** Part 8, Physical Security Plan, Section 4.1, Security Organization Management (Page 4), Training and Qualification Plan, Section 3.3, Critical Task Matrix (Pages B-7, B-15 through B-19 and Contingency Plan, Section 4.1. License Organization (Pages C-17 through C-19): Clarify and indicate the difference, if any, between the individual that is designated and defined as "Response Team Leader (RTL)," and the individual designated as "Response Force Leader (RFL)." Provide consistent use of either RFL or RTL in referring to the same individual.

(U) Regulatory Basis: Title 10 CFR 52.6, Completeness and accuracy of information, requires information provided "shall be complete and accurate in all material respects." The applicant uses "RTL" in the PSP and use "RFL" in the remaining two plans submitted under Part 8 of the application.

ANSWER:

The correct term is Response Force Leader (RFL), as opposed to Response Team Leader (RTL). *The PSP Section 4.1 will be revised to use the term Response Force Leader (RFL).*

Impact on R-COLA

The PSP will be revised in the next COLA revision.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-24

24. **(U)** Part 8, Physical Security Plan, Section 11, Physical Barriers (Pages 8-13): Indicate reference to MHI Technical Report UAP-SGI-08002, Revision 1, US-APWR High Assurance Assessment Evaluation Report, that addresses detailed descriptions of design and performance requirements of physical barriers - or - clarify what parts of the COL application addresses or incorporates the MHI Technical Report UAP-SGI-08002 that describes the details for the design of physical barriers described in Section 11.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to provide capabilities to detect, assess, interdict, and neutralize the DBT and maintain at all time such capabilities. The design of physical protection systems beyond the scope of the DC is required as COL Information Item 13.6.1. Title 10 CFR 52.6, Completeness and accuracy of information, requires information provided "shall be complete and accurate in all material respects." Title 10 CFR 52.80(a) required the application to contain information for ITA and criteria necessary and sufficient to provide reasonable assurance that the facility has been constructed and will operate in conformity with the combined license, the provisions of the Act, and the Commission's rules and regulations. MHI Technical Report UAP-SGI-08002 R1, U.S. APWR - High Assurance Assessment Evaluation Report, addresses the detailed descriptions of design and performance requirements that are intended to conform to guidance of RG 1.206 for a COL application. The applicant did not incorporate by reference the portions of the MHI Technical Report UAP-SGI-08002, which contain the design of physical protection systems within the scope of the COL applicant.

ANSWER:

See the response to Question 13.06.01-1 above, which states that the HAE, including Appendix A, is described in FSAR Section 13.6. This response also identifies that CPNPP is the reference plant for these assessments and that the design descriptions and performance requirements attributed to the reference plant apply to CPNPP 3 and 4.

Impact on R-COLA

None.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-25

25. **(U)** Part 8, Physical Security Plan, Section 11.2, Vehicle Barriers (Pages 9 and 10): Indicate references to documents (e.g., MHI UAP-SGI-080002 or others) containing the analyzed results, analysis assumptions, and methods or approaches used, and technical basis for determining adequate stand off distance(s) for the vehicle bomb threats described in Sections 11.2.1 and 11.2.2.

(U) Regulatory Basis: Subpart B of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT. Title 10 CFR 52.6, Completeness and accuracy of information, requires information provided "shall be complete and accurate in all material respects." The applicant states that "[a] site-specific analysis has been conducted and physical barriers are [will be] used where appropriate in the OCA, PA, and VAs to perform any or more of the following functions . . (7) protect the personnel, systems, and equipment needed to prevent . . . sabotage against a vehicle bomb . . ." Section 11.2 does not describe the minimum required stand off distance(s) for the design of the VBS or provide the supporting licensing basis for adequate minimum stand off distance(s) that protecting against the DBT vehicle bomb(s). The reference to technical report and specific blast analysis that contains the technical basis and a summary of results supporting the applicant statements of adequate protection against vehicle bombs may be addressed in Part 2, FSAR Chapter 13.6 and/or incorporated by reference.

ANSWER:

UAP-SGI-10002, Rev. 0 and UAP-SGI-10003, R0 provide the minimum safe standoff distances for vehicle bombs identified in the DBT. These reports are applicable to CPNPP Units 3 and 4 in that they specifically address the US-APWR design and the CPNPP Units 3 and 4 site-specific designs.

Impact on R-COLA

None.

Impact on S-COLA

None.

Impact on DCD

UAP-SGI-08002, High Assurance Evaluation Assessment, Appendix A, Rev. 1, will be revised to reference UAP-SGI-10002, Rev. 0 and UAP-SGI-10003, R0.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-26

26. **(U)** Part 8, Physical Security Plan, Section 11.2, Vehicle Barriers (Page 9): Clarify and indicate the specific design and performance requirements for meeting what is considered an "acceptable level" in the statement that the "[r]oad layout up to the active barriers is designed to reduce the force of the moving vehicle to an acceptable level." Confirm that the design and performance requirements of the physical protection systems applied the bounding vehicle size and maximum speed of the DBT.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT and maintain at all time such capabilities. Title 10 CFR 52.80(a) required the application to contain information for ITA and criteria necessary and sufficient to provide reasonable assurance that the facility has been constructed and will operate in conformity with the combined license, the provisions of the Act, and the Commission's rules and regulations. Title 10 CFR 52.6, Completeness and accuracy of information, requires information provided "shall be complete and accurate in all material respects." The design performance requirement of "acceptable level" must be sufficiently described for verification by inspections, test, or analysis of the engineered features that will be designed and constructed. Specific design and performance requirements must be sufficiently describe for verification and assurance of adequate protection.

(U) Note: The information addressing specific details related to security features or providing security functions will be safeguards information (SGI) and should be marked and protected in accordance with 10 CFR 73.21. The applicant should portion mark text in the response to request for additional information (RAI) as appropriate to identify SGI (or Official-Use-Only Security-Related Information) that reveals the specific details of physical protection.

ANSWER:

The Vehicle Barrier System at CPNPP Units 3 and 4 is designed, constructed, installed, and maintained to protect the facility against the DBT. It includes an integrated system of passive and active barriers that would withstand explosives and stop a DBT vehicle. *Thus the sentence "Road layout up to the active barriers is designed to reduce the force of the moving vehicle to an acceptable level" is unnecessary and will be deleted from the PSP.*

Impact on R-COLA

The PSP Section 11.2.1 will be revised in the next COLA revision.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-27

27. **(U)** Part 8, Physical Security Plan, Section 11.2.3, Waterborne Threat Measures (Page 11): Indicate reference to the technical report or document that contains the site-specific analysis providing the technical and licensing basis supporting the conclusions in this section that the ". . . (closest vital equipment) and remaining vital equipment buildings have been analyzed for blast and found to be acceptable for performing their functions."

(U) Regulatory Basis: Subpart B of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT. Title 10 CFR 73.1(1)(E)(iv) requires protection against the DBT waterborne vehicle bomb. Title 10 CFR 52.6, Completeness and accuracy of information, requires information provided "shall be complete and accurate in all material respects." The applicant stated that it has analyzed (i.e., documented) for blast and provided an adequate protection. The blast analysis providing the applicant technical basis of adequate protection must be incorporated by reference for completeness of licensing basis and a summary of analysis result must be provided in the COL application to demonstrate how it met regulatory requirements of 10 CFR 73.1(E)(iv).

(U) Note: The information addressing specific details related to security features or providing security functions will be safeguards information (SGI) and should be marked and protected in accordance with 10 CFR 73.21. The applicant should portion mark text in the response to request for additional information (RAI) as appropriate to identify SGI (or Official-Use-Only Security-Related Information) that reveals the specific details of physical protection.

ANSWER:

See the response to Question 13.06.01-25. *UAP-SGI-10003, R0 will be referenced in the HAE Appendix A, Rev. 1 and will be revised to clearly indicate that the waterborne threat is encompassed in the analysis.*

Impact on R-COLA

None.

Impact on S-COLA

None.

Impact on DCD

UAP-SGI-08002, High Assurance Evaluation Assessment, Appendix A, will be revised to reference UAP-SGI-10003, R0 discussed in this response.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-28

28. **(U)** Part 8, Physical Security Plan, Section 11.3, Protected Area Barriers (Page 11): Provide descriptions of design requirements of the physical protection systems that will provide continuity of the detection of penetrations above the Access Control Building (ACB) and building penetrations (including doors, HVAC, and windows) of the ACB that serves as a portion of the PA barrier. Include in the response, clarify whether fencing, as described is a design requirement on the roof of the ACB.

(U) Regulatory Basis: Subpart B of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT. The design of the ACB serving as part of the PA barrier must include capabilities for detection. The design of ACB did not describe capabilities of detecting attempted penetrations of the portion of the ACB structure that will serve the PA barrier.

(U) Note: The information addressing specific details related to security features or providing security functions will be safeguards information (SGI) and should be marked and protected in accordance with 10 CFR 73.21. The applicant should portion mark text in the response to request for additional information (RAI) as appropriate to identify SGI (or Official-Use-Only Security-Related Information) that reveals the specific details of physical protection.

ANSWER:

High Assurance Evaluation Assessment, Appendix A, Rev. 1, will be revised as necessary to include the design requirements of the physical protection systems that will provide continuity of the detection of penetrations above the Access Control Building (ACB) and building penetrations (including doors, HVAC, and windows) of the ACB. This will include fencing as necessary. CPNPP Units 3 and 4 is the reference plant for these assessments. Therefore, the design descriptions and performance requirements attributed to the reference plant apply to CPNPP Units 3 and 4.

Impact on R-COLA

None.

Impact on S-COLA

None.

Impact on DCD

UAP-SGI-08002, High Assurance Evaluation Assessment, Appendix A, Rev. 1, will be revised as necessary to include the design requirements of the physical protection systems that will provide continuity of the detection of penetrations above the Access Control Building (ACB) and building penetrations (including doors, HVAC, and windows) of the ACB. This will include fencing as necessary.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-29

29. **(U)** Part 8, Physical Security Plan, Section 11.3, Protected Area Barriers (last sentence, Page 12): Describe the design requirements of engineered systems or features that will be established to "limit the potential for an unauthorized train to penetrate the protected area boundary." In addition, describe if the design and performance requirements for the assessment systems (CCTV or others) provided, including capabilities to provide surveillance to verify conditions and availability of the "measure" provided.

(U) Regulatory Basis: Subpart B of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT. Title 10 CFR 52.6, Completeness and accuracy of information, requires information provided "shall be complete and accurate in all material respects." The applicant states that "[m]easures have been established" to limit potential for an unauthorized train to penetrate the PA. Section 11.3 did not describe the system or feature and the design requirements to perform the intended function of stopping or preventing a train. The reference to technical report that contains descriptions design and performance requirements of physical protection systems may be addressed in Part 2, FSAR Chapter 13.6 and/or appropriate reference to MHI UAP-SGI-080002.

(U) Note: The information addressing specific details related to security features or providing security functions will be safeguards information (SGI) and should be marked and protected in accordance with 10 CFR 73.21. The applicant should portion mark text in the response to request for additional information (RAI) as appropriate to identify SGI (or Official-Use-Only Security-Related Information) that reveals the specific details of physical protection.

ANSWER:

The train tracks located on the Owner Controlled Area will terminate outside the Protected Area for CPNPP Units 3 and 4 at a such distance that a train will not be capable of reaching the Protected Area. In addition, the tracks will have derailers installed and will have portions of the rail system removed to further limit the train from reaching the Protected Area boundary. With these measures in place, CCTV camera capabilities are not required, although periodic surveillance measures of the train tracks will be implemented. *The PSP, Section 11.3, will be revised to address adding a derailer and the removal of a section of track in accordance with 10 CFR 73.55(e)(10)(i)(D).*

Impact on R-COLA

The PSP will be revised in the next COLA revision.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-30

30. **(U)** Part 8, Physical Security Plan, Section 11.3, Protected Area Barriers (Page 11): Provide descriptions of the types of "interior security features" (i.e., engineered systems) for performing PA packages and material searches described in the Section 14.4.2 and personnel search described in Section 14.4.4. Specifically address whether descriptions for the maintenance of search equipment in Section 20.2, Search Equipment, are the types of interior security features that will be incorporated by design to meet requirements for search of packages, material, and persons.

(U) Regulatory Basis: Subpart B of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT. The description of interior security features must include, in general, the types of engineered systems or technologies that will be provided for search of packages, material, and personnel. Section 14.4.2, and 14.4.4 states that special purpose detector or equipment capable of detecting firearms, explosives, incendiary devices or other items used to commit radiological sabotage are provided to conduct searches, along with the option of conducting physical search.

(U) Note: The information addressing specific details related to security features or providing security functions will be safeguards information (SGI) and should be marked and protected in accordance with 10 CFR 73.21. The applicant should portion mark text in the response to request for additional information (RAI) as appropriate to identify SGI (or Official-Use-Only Security-Related Information) that reveals the specific details of physical protection.

ANSWER:

The PSP, Subsections 14.4.2 and 14.4.4 will be revised to identify the types of equipment that will be used for material and personnel searches, respectively. The types of search equipment used will correspond to the equipment types identified in Section 20.2.

Impact on R-COLA

The PSP will be revised in the next COLA revision.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-31

31. **(U)** Part 8, Physical Security Plan, Section 14.2, Insider Mitigation Program (Page15): Clarify whether the statement "utilizing the guidance provided in Regulatory Guide 5.75" means implementing the insider mitigation program in accordance with all portions of referenced Regulatory Guide 5.77, Insider Mitigation Program, that would provide a licensing basis for how Luminant will meet 10 CFR 73.55(a)(9).

(U) Regulatory Basis: Subpart B of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for combined license (COL) include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(a)(9) requires an applicant to provide program and physical protection against insider threat, as characterized by the adversarial characteristics of the design basis threat. Regulatory Guide 5.77, Insider Mitigation Program, provide guidance that may be applied for meeting regulatory requirements on mitigating insider threat.

ANSWER:

The correct citation for 10 CFR 73.55 is 10 CFR 73.55(b)(9). The correct Regulatory Guide referenced in PSP Section 14.2 on page15 is RG 5.77.

The text in PSP Section 14.2 that says, "utilizing the guidance in RG 5.77" is black letter text in the NEI 03-12 template that is generically applicable to all plants using the template. Black letter text is verbatim language from the NRC-endorsed NEI 03-12, Revision 6 template. There are no site-specific conditions that would make this black letter text inapplicable to CPNPP Units 3 and 4; therefore, the NRC endorsed-text remains unchanged for CPNPP Units 3 and 4. Luminant understands that the NRC and NEI are currently discussing revisions to be made to the NEI template, which would be issued as Revision 7. CPNPP programs are revised to address updates to NRC-endorsed templates as appropriate.

Impact on R-COLA

None.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-32

32. **(U)** Part 8, Physical Security Plan, Section 14.2, Insider Mitigation Program (last sentence, Page 15): Provide justifications and technical bases for the proposed "alternative methodology" described in Section 14.2 as it relates to the "fuel pool." Identify clearly the specific regulatory requirement(s) of 10 CFR 73 that this alternative methodology is intended to address. Provide a specific request of alternate measure for review and approval in accordance with 10 CFR 73.55(r).

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT and maintain at all time such capabilities. Title 10 CFR 73.55(r), Alternative measures, requires an applicant to submit technical basis for the proposed alternative measure(s) to the Commission for review and approval. In the case of a COL applicant, the applicant proposed alternative measure is reviewed during review of the applications, prior to issuance of a license. Section 14.2 includes a proposed an alternative without specifying the regulation and did not provide detailed descriptions of alternative measures and justifying technical basis. The application of NRC accepted industry template NEI 03-12 for submitting security plans is guidance and conformance to the NEI template is not a justification for alternative to or a noncompliance with regulatory requirements. Any alternative to regulatory requirements of 10 CFR 73 in the application must be addressed under 10 CFR 73.55(r).

(U) Note: The information addressing specific details related to security features or providing security functions will be safeguards information (SGI) and should be marked and protected in accordance with 10 CFR 73.21. The applicant should portion mark text in the response to request for additional information (RAI) as appropriate to identify SGI (or Official-Use-Only Security-Related Information) that reveals the specific details of physical protection.

ANSWER:

Page 15 of PSP Section 14.2 provides an alternate method for the patrols to those identified in the PSP for stand-alone target set equipment. This alternate method does not pertain to the regulatory requirements in 10 CFR 73.55(i)(5)(vi), which states that the licensee shall provide random patrols of all accessible areas containing target set equipment. Section 14.2 of the PSP establishes the frequency of the random patrols for areas containing target set equipment which is maintained to meet the regulatory requirements in the 73.55(i)(5)(vi). There is no alternate method to the regulatory requirements and 10 CFR 73.55(r) does not apply to the alternate methodology for monitoring the fuel pool as described in Section 14.2 of the PSP.

Impact on R-COLA

None.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-33

33. **(U)** Part 8, Physical Security Plan, Section 14.5, Vital Area Access Control (6th bullet, Page 21): Clarify and indicate the design and performance requirements associated with the two class (or types) of alarm supervision indicated in the 6th bullet. In addition, describe what portions of the intrusion detection and alarm system and components will be designed to meet a particular class of supervision stated and describe the specific industry or consensus that establishes the standard for providing the supervision functions.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT. The 6th bullet describing the design and performance requirements for intrusion alarm system identify a choice of two types of alarm line supervision. Clarification is requested to explain what is specifically required for design and that applicant's assumptions for each of the class of supervision and what industry standard are applied (e.g., NFPA 72, UL standard, Factory Mutual, or others).

(U) Note: The information addressing specific details related to security features or providing security functions will be safeguards information (SGI) and should be marked and protected in accordance with 10 CFR 73.21. The applicant should portion mark text in the response to request for additional information (RAI) as appropriate to identify SGI (or Official-Use-Only Security-Related Information) that reveals the specific details of physical protection.

ANSWER:

Interim Federal Specification W-A-00450B (GSA-FSS), dated 2/16/73, is referenced in UAP-SGI-08002, High Assurance Evaluation Assessment, Appendix A, and describes the different classes for circuit supervision. CPNPP Units 3 and 4 will use Class A supervision for digital and tone-wire transmitted

circuits as applicable, and will use Class B supervision for AC or DC wire transmitted circuits as applicable.

Impact on R-COLA

None.

Impact on S-COLA

None.

Impact on DCD

UAP-SGI-08002, High Assurance Evaluation Assessment, Appendix A, Rev. 1, will be revised to state that CPNPP Units 3 and 4 will use Class A supervision for digital and tone-wire transmitted circuits as applicable, and will use Class B supervision for AC or DC wire transmitted circuits as applicable.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-34

34. **(U)** Part 8, Physical Security Plan, Section 14.5, Vital Area Access Control (Page 21): Describe the design and performance requirements for interior intrusion detection systems (IDS) and alarms for detecting unauthorized access to vital areas (VA). Specifically, address the following: (a) describe the assumptions regarding detecting unauthorized access through other than VA normal and emergency access points (i.e., other penetrations); (b) describe how other penetrations or openings would be locked and alarmed; (c) describe, if any, assumptions for a maximum size of openings or penetrations in the VA barriers would not required physical barrier and alarmed; and (d) describe how the interior IDS will be integrated with the internal surveillance system for assessment.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT and maintain at all time such capabilities. Title 10 CFR 73.55(b)(9)(ii) and (iii) requires openings in VA barriers to be alarmed for detection of unauthorized access. The MHI Technical Report UAP-SGI-080002 technical contains descriptions design and performance requirements of physical protection systems that are described in Part 2, FSAR Chapter 13.6 and may be incorporated by reference.

(U) Note: The information addressing specific details related to security features or providing security functions will be safeguards information (SGI) and should be marked and protected in accordance with 10 CFR 73.21. The applicant should portion mark text in the response to request for additional information (RAI) as appropriate to identify SGI (or Official-Use-Only Security-Related Information) that reveals the specific details of physical protection.

ANSWER:

(a, b, c) The DCD and sections of UAP-SGI-08002, High Assurance Evaluation Assessment, Rev. 1, describe measures taken to lock and alarm VAs that are within the US-APWR standard plant.

In accordance with NRC guidance, openings or penetrations that are less than 96 sq-in are not locked or alarmed. The 96-sq-in threshold for locking and alarming VA penetrations applies to COLA-related VAs.

(d) Interior IDS alarms are displayed in the CAS and SAS. Upon an alarm associated with a VA barrier, one or more security officers are dispatched to the location to assess the alarm. CCTV cameras may also be used to provide assessment of alarms.

Impact on R-COLA

None.

Impact on S-COLA

None.

Impact on DCD

UAP-SGI-08002, High Assurance Evaluation Assessment, Appendix A, Rev. 1, will be revised for reference plant vital area's to incorporate the 96-sq-in rule.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-35

35. **(U)** Part 8, Physical Security Plan, Section 14.5, Vital Area Access Control and Section 16.2 System Description (7th bullet, Page 21 and last paragraph, Page 27): Clarify and indicate whether the standby power described in the first sentence (with capabilities as indicated) is in addition to backup power indicated in the last sentence. Include in the following in the RAI response: (a) indicate whether an uninterruptable power supply (UPS) is incorporated in the design to provide continuity of IDS functions without interruption between loss of off-site power and the availability of power from the standby and/or backup power system(s); (b) Indicate the technical basis for the adequacy of the minimum hours indicated for the design of standby power; (c) clarify whether surveillance system is provided in the design for assessment of the vital areas (e.g., similar to selected capabilities described in Section 15); and (d) clarify whether "emergency power system" in Section 6.2 for security communications is the same as "standby power" described in Section 14.5.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT and maintain at all time such capabilities. The reliability and availability of IDS to continue performing its intended functions up on the lost of primary power is required to initiate assessment and response to protect the plant against the DBT. Clarification is required for identified power supply and the licensing basis for adequate detection capabilities to initiate assessment and response. Section 15, Surveillance Observation and Monitoring, describes UPS that appears to be limited to the IDS and surveillance systems for areas outside of the VA. The application contain different terms for describing the source of secondary power and clarification is needed for the system(s) that will be provided for assure continuity of physical protections systems functions upon loss of primary power.

(U) Note: The information addressing specific details related to security features or providing security functions will be safeguards information (SGI) and should be marked and protected in accordance with 10 CFR 73.21. The applicant should portion mark text in the response to request for additional information

(RAI) as appropriate to identify SGI (or Official-Use-Only Security-Related Information) that reveals the specific details of physical protection.

ANSWER:

[

]

The PSP will be revised to ensure consistency in the use of backup and standby power.

Impact on R-COLA

The PSP will be revised in the next COLA revision.

Impact on S-COLA

None.

Impact on DCD

Section 13.6.2.6 of the DCD and the applicable subsections of Section 5 of the HAE will be similarly revised to provide consistency in the use of backup and standby power.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-36

36. **(U)** Part 8, Physical Security Plan, Section 14.5, Vital Area Access Control (6th bullet, Page 22): Verify the consistency between the listed vital areas on Page 22 of the PSP and the designations of vital areas in Appendix E of MHI Technical Report UAP-SGI-08001, Revision 2, dated December 2009, that is incorporated by reference.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT and maintain at all time such capabilities. Title 10 CFR 52.6, Completeness and accuracy of information, requires information provided "shall be complete and accurate in all material respects." The DCD, referenced technical report, MHI Technical Report UAP-SGI-08001 identifies vital areas in Appendix E. Figure 11, appears to identify additional vital areas that are not described in Section 14.5. The vital areas described in the PSP and those described and shown on figures of the DCD referenced MHI Technical Report UAP-SGI-08001 must be consistent.

ANSWER:

[

]

Impact on R-COLA

The PSP will be revised in the next COLA revision.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-37

37. **(U)** Part 8, Physical Security Plan, Section 15.4, Central Alarm Station (CAS) and Secondary Alarm Station (SAS) Operations (3rd paragraph, Page 24): Describe the design and performance of physical security systems that will reside within CAS and SAS. Include the following in the response: (a) descriptions of design and performance requirements, a conceptual design block diagram of systems and components within the CAS and SAS and their interfaces with plant systems (public announcement system, emergency exits, access control features, active barriers, primary and secondary power, etc.); (b) the interfaces between CAS and SAS; and (c) a summary of evaluation and resulting design and performance requirements, including crediting spatial separation, to provide protection against single act that could lead to loss of security functions of both the CAS and SAS.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT and maintain at all time such capabilities. Title 10 CFR 73.55(i)(4)(i) and (iii) requires design against single act the can disable both alarm stations and provisions for equal and redundant CAS and SAS. The descriptions design and performance requirements of physical protection systems may be addressed in Part 2, FSAR Chapter 13.6 and/or appropriate reference to MHI UAP-SGI-080002.

(U) Note: The information addressing specific details related to security features or providing security functions will be safeguards information (SGI) and should be marked and protected in accordance with 10 CFR 73.21. The applicant should portion mark text in the response to request for additional information (RAI) as appropriate to identify SGI (or Official-Use-Only Security-Related Information) that reveals the specific details of physical protection.

ANSWER:

(a, b) See the response to Question 13.06.01-9 above.

(c) The CAS for CPNPP Units 3 and 4 will be located in an interior location in Unit 3 and the SAS will be located in an interior location in Unit 4. There will be substantial physical and structural separation between the two alarm stations such that the DBT at the VBS will not disable either the CAS or SAS. This physical separation, in concert with the redundant functionality discussed in (a) and (b) above, ensures that no single adversary act could lead to loss of security functions for both the CAS and SAS.

Impact on R-COLA

None.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-38

38. **(U)** Part 8, Physical Security Plan, Section 18, Response Requirements (Page 29) and Safeguards Contingency Plan, Section 8, Protective Strategy (2nd paragraph, Page C-25): Clarify whether the number of "additional armed security offices (ASO) on site that are available at all times to respond" are dedicated to CPNPP Units 3 and 4 - or - whether they are available for all reactors, operating CPNPP Units 1 and 2 and CPNPP Units 3 and 4. If the indicated ASO are available for protection of all reactor units, address the following: (a) indicate the distribution of ASO between the new and operating units under full power operations, refueling outage, and under heighten threat environment of imminent attack; (b) describe how the responses of ASO were considered based on distributions of ASO between operating and new units; (c) describe how the ASO will be deployed and how engineered systems relied on to implement response to deny adversaries access to the VA; (d) discuss whether the ASO response include pursuit of adversaries; and (e) describe measures considered to address friendly fire in implementing pursuit portion of the strategy. If the number of ASO are dedicated to Units 3 and 4 only, (f) provide supplemental information to MHI Technical Report UAP-SGI-08002, R1 on how they are applied or supplement the numbers of responders and responses to postulated bounding adversaries scenarios described in MHI Technical Report; and (g) what engineered physical protection systems or features (e.g., fighting positions and strategic placements) are relied and technical basis that provides tactical advantages for the ASO.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT and maintain at all time such capabilities. Title 10 CFR 73.55(b)(ii) requires defense-in-depth through integration of engineered and administrative controls for effective physical protection. Clarification is required to establish clearly the assumptions for availability of ASO as described in Section 18 of the PSP and the statements of the Safeguards Contingency Plan (2nd paragraph, Page C-25) that the "two facility [CPNPP Units 1 and 2 and CPNPP Units 3 and 4] security plans are not contingent upon providing support to each other."

(U) Note: The information addressing specific details related to security features or providing security functions will be safeguards information (SGI) and should be marked and protected in accordance with 10 CFR 73.21. The applicant should portion mark text in the response to request for additional information (RAI) as appropriate to identify SGI (or Official-Use-Only Security-Related Information) that reveals the specific details of physical protection.

ANSWER:

(a - f) As stated in the PSP, all additional ASOs are dedicated to the CPNPP Units 3 and 4 response. There is no sharing of ASO resources with CPNPP Units 1 and 2.

(g) Fighting positions and their strategic placements for ASOs are established as part of the implementation of the physical security program, which is a license condition.

Impact on R-COLA

None.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-39

39. **(U)** Part 8, Training and Qualification Plan, Section 3.6.4, Firearms Qualification Courses and Section 3.6.4.1, Course of Fire (Pages B-12): Remove reference to enhanced weapons.

(U) Regulatory Basis: The training and qualification plan indicates qualification for weapon and courses of fire on "enhanced weapons." Current NRC regulation does include or authorize the use of enhanced weapons. Rulemaking is under consideration by the Commission, and the use of enhanced weapon is not yet authorized. In addition, Section 9.0 of the Physical Security Plan does not specify or plans for the use of enhanced weapons.

ANSWER:

The text in Section 3.6.4.1 is black letter text in the NEI template that would be generically applicable to all plants using the template upon NRC authorization for enhance weapons. Black letter text is verbatim language from the NRC-endorsed NEI 03-12, Revision 6, template. There are no site-specific conditions that would make this black letter text inapplicable to CPNPP Units 3 and 4; therefore, the NRC-endorsed text remains unchanged for CPNPP Units 3 and 4. The description in Section 3.6.4 of firearms qualification courses for enhanced weapons provides qualification requirements if and when the NRC authorizes the use of enhanced weapons. Luminant understands that the NRC and NEI are currently discussing revisions to be made to the NEI template, which would be issued as Revision 7. CPNPP programs are revised to address updates to NRC-endorsed templates as appropriate.

Impact on R-COLA

None.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-40

40. **(U)** Part 8, Physical Security Plan, Safeguards Contingency Plan, Section 4.1.1, Duties/Communications Protocols and Section 4.1.2, Security Chain of Command/Delegation of Authority (Pages C-17 and C-18): Reconcile the term "Response Force Leader" and "Armed Response Team Leader" (Security Shift Supervisor Qualified)" indicated Section 4.1, Security Organization Management, on Page 4 of the PSP.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT and descriptions of implementation of the physical security plan. Title 10 CFR 52.6, Completeness and accuracy of information, requires information provided "shall be complete and accurate in all material respects." The applicant uses different terms for describing the same security position.

ANSWER:

As stated in the response to Question 13.06.01-23 to this RAI, the "Response Force Leader" is the correct title for security official responsible for directing the security force in effecting a protective strategy.

Impact on R-COLA

None.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-41

41. **(U)** Part 8, Safeguards Contingency Plan, Section 4.1.2, Security Chain of Command/ Delegation of Authority (Page C-18) and T&Q Plan, Table 1 (Page B-15 to B-24): Provide appropriate revision to training requirements for CAS and SAS operators in the T&Q Plan, Table 1, Critical Task Matrix, Pages B-15 to B-24, to justify that the CAS or SAS operators would be qualified to fulfill the chain of command as a RFL during a security contingency event. In addition, provide clarification and justifications of how the CAS or SAS operators assigned duties of alarm responses, assessments, and communications (e.g., providing redundancies of functions and performing internal and external interface requirements) will perform RFL responsibilities at the same time. Clarify when or under what conditions would a CAS or SAS operator may take on succession of chain of command as stated in Section 4.1.2 without interfering with performing alarms, assessments, and communications responsibilities.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for combined license (COL) include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT and descriptions of implementation of the physical security plan. Title 10 CFR 52.6, Completeness and accuracy of information, requires information provided "shall be complete and accurate in all material respects." Section 4.1.2 indicates that the CAS or SAS Operator may assume command and control if the RFL is unavailable. The Training Matrix in Appendix B did not include all training tasks that would provide assurance that a CAS or SAS Operator would be appropriately trained and qualified to command and control of the security response (i.e., qualified as a RFL). Clarification and justifications are needed regarding when a CAS or SAS operator may take on succession of chain of command when the RFL is unavailable as stated in Section 4.1.2 (i.e., without interfering with performing alarms, assessments, and communications responsibilities).

(U) Note: The information addressing specific details related to security features or providing security functions will be safeguards information (SGI) and should be marked and protected in accordance with 10 CFR 73.21. The applicant should portion mark text in the response to request for additional information

(RAI) as appropriate to identify SGI (or Official-Use-Only Security-Related Information) that reveals the specific details of physical protection.

ANSWER:

The T&Q Plan Critical Task Matrix, page B-18, Task 21, currently indicates that the CAS and SAS operators can perform the role of the RFL and would be trained accordingly. Section 4.1.2 of the Contingency Plan identifies the conditions under which the CAS or SAS operator would assume direction of response force activities, i.e., in the event the RFL is no longer able to perform the function as the RFL. Notably, these command and control responsibilities would be carried out in the CAS or SAS, as applicable, rather than elsewhere on site. Any event in which the CAS or SAS operator assumes command would be considered an extraordinary security event, likely associated with a hostile adversary attack on the plant. Under such extreme conditions and in the absence of the normal RFL, an appropriately-trained CAS or SAS operator is in a position to assess unfolding events via the CAS/SAS detection, assessment, communications, and response equipment; provide direction to remaining response forces; and coordinate with arriving off-site response forces. During an event requiring the CAS or SAS operator to assume RFL command duties, all attention and energy will be focused on resolving the security situation, which is consistent with the usual duties of an alarm station operator, such as detection, assessment, and control of active barrier systems. Accordingly, assumption of RFL functions by an alarm station operator would constitute an intensification of alarm station operator activity, rather than a distraction from normal activities.

Impact on R-COLA

PSP Section 4.1.2 will be revised to add "no longer able to perform the function as the RFL" in the next COLA revision.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-42

42. **(U)** Part 8, Safeguards Contingency Plan, Section 4.3, Safeguards Systems (Page C-19): Clarify whether the "design documents" stated include the MHI Technical Report UAP-SGI-80002 that describes the design and performance requirements and licensing bases that will be referenced or submitted with Part 8 of the application. Provide definition of "Safeguards Systems," to clarify the difference between "Physical Protection System" as used in Section 2, Performance Objective of the PSP (Page 2) and "safeguards systems."

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT and maintain at all time such capabilities. Title 10 CFR 52.6, Completeness and accuracy of information, requires information provided "shall be complete and accurate in all material respects." The applicant states that "[s]afeguards systems are described in Section 9, 11, 12, 13, 15, and 16 or the PSP, and in facility implementation procedures/design documents." Clarification is needed on whether MHI UAP-SGI-80002 containing descriptions of design and performance requirements and design basis for physical protection system (i.e., detection, assessment, delay and response) is consider a design document.

ANSWER:

As stated in the response to Question 13.06.01-1, the licensing basis design performance requirements described in the HAE will be incorporated and maintained in plant-specific supporting documents including design documents, procedures, and records. These supporting engineering documents and drawings will be the design documents that are referenced in Section 14.3 of the Safeguards Contingency Plan.

The terms “physical security systems” and “safeguards systems” are used synonymously throughout the PSP and Contingency Plan.

Impact on R-COLA

None.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-43

43. **(U)** Part 8, Safeguards Contingency Plan, Section 7, Primary Security Functions (3rd paragraph, Page C-23): Describe the types of facility procedures that will contain the "process for the oversight of target set equipment and systems to ensure that changes to configuration of identified safety-related equipment and system are considered in the site protective strategy," as stated for change controls and how the safety/security interface will be addressed.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT and 10 CFR 73.55(h) requires maintaining reliable and available search capabilities of persons and materials at all time. Target sets (safety structures, systems and components) are identified by the applicant in accordance with 10 CFR 73.55(f) are SSC that the applicant will protect based on the DBT. Title 10 CFR 73.58 requires management of safety/security interface to ensure changes affecting security and the applicant must describe how it manages the interface. Target sets are safety-related structures, systems and components and/or operational related administrative controls that must be maintained updated based on configuration changes to plant systems and equipment.

ANSWER:

See the response to Question No. 13.06.01-18.

Impact on R-COLA

See answer to Question No. 13.06.01-18.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-44

44. **(U)** Part 8, Safeguards Contingency Plan, Section 7, Primary Security Functions (6th paragraph, Page C-24): Provide clarification and confirm the accuracy of the statement that the state (i.e., Texas Department of Public Safety (DPS)) is the "primary command and control organization." Include the following in the RAI responses: (a) provide justification of why the lead federal response agency (i.e., Federal Bureau of Investigation), identified in Section 5.8, would not be the lead law enforcement agency for a terrorist event, once it arrive on site; (b) why the applicant commits the Texas DPS the requirement that it "shall implement the necessary actions to recovery from the contingency and return to normal operations" of the CPNPP Units 3 and 4, and (c) describe how Texas DPS formally commits and provide assurance it will met the requirements as stated in this Section.

(U) Regulatory Basis: Title 10 CFR 52.6, Completeness and accuracy of information, requires information provided "shall be complete and accurate in all material respects." The licensee is responsible for both the safety and security of the licensed facility at all times. In a terrorist event, the FBI is the lead federal agency for response to terrorist events at any federal or state licensed facilities. The lead law enforcement agency is the FBI, and it would lead the incident command for both the response to the threat that has not been neutralized and the criminal investigation afterwards, with the support of licensee security personnel and the state and local law enforcement organizations (including Texas DPS). Clarification, and confirmation, is needed for the statement that the Texas DPS will be the lead "command and control" organization for either security or safety.

(U) Note: The information addressing specific details related to security features or providing security functions will be safeguards information (SGI) and should be marked and protected in accordance with 10 CFR 73.21. The applicant should portion mark text in the response to request for additional information (RAI) as appropriate to identify SGI (or Official-Use-Only Security-Related Information) that reveals the specific details of physical protection.

ANSWER:

(a, b) The DPS, identified in Section 8, Protective Strategy, as a first responder, is the primary command and control organization and is the logical LLEA responder available to direct security operations until the point when normal operations can be restored. However, if the event is determined to be a terrorist event or another violation of federal law, then the FBI would be the lead organization for subsequent investigation and after-actions.

(c) There is a Memorandum of Understanding between Luminant and the DPS that identifies the commitments to which the DPS has agreed to, and this is reviewed and updated annually.

Impact on R-COLA

None.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-45

45. **(U)** Part 8, Safeguards Contingency Plan, Section 8, Protective Strategy (1st paragraph,9th line, Page C-25): Clarify whether the stated "Security Officers (SOs)" should be "Armed Responders (AR)" as described in Section 18, Response Requirements, on page 29 of the PSP.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for combined license (COL) include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT and maintain at all time such capabilities. Armed Security Officers are credited in implementing the site protective strategy in the PSP. The term "Security Officer" is not defined in Appendix A of the PSP and the term "Supplemental Security Officers" are not required or relied on for immediate response.

ANSWER:

The wording in the Safeguards Contingency Plan, page C-25, 1st paragraph, 4th sentence, will be revised to refer to Armed Security Officers (ASOs)/Armed Responders (ARs)" The Safeguards Contingency Plan, Section 8, will be revised to appropriately use this terminology.

Impact on R-COLA

The Safeguards Contingency Plan will be revised in the next COLA revision.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-46

46. **(U)** Part 8, Safeguards Contingency Plan, Section 8, Protective Strategy (3rd paragraph, 2nd to last sentence, Page C-25): Describe the design and performance requirements for the interface of the Units 3 and 4 engineered system (as indicated) to the Units 1 and 2 Secondary Alarm Station. Include the description for the following in the RAI response: (a) the intended purpose for requiring the engineered systems control interfaces between the two facilities; (b) the required assessments and communications capabilities to perform the intended functions; (c) the design requirements for assuring the integrity of actuation signal (including line supervisions, alarm indications, trouble conditions, etc.) from the locations of the engineered systems from Units 3 and 4 to the Secondary Alarm Station for Units 1 and 2, through the OCA; (d) clarify whether the same functions are provided within the CAS for CPNPP Units 3 and 4; and (e) describe how requirements for redundancy of functions are provided in the SAS of CPNPP Units 3 and 4.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for combined license (COL) include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT and maintain at all time such capabilities. Clarification is required of the intended purpose for requiring support from Units 1 and 2 for a physical protection system protecting the proposed CPNPP Units 3 and 4. The configuration proposed must be designed with assurance that the intended functions will be reliable and available.

(U) Note: The information addressing specific details related to security features or providing security functions will be safeguards information (SGI) and should be marked and protected in accordance with 10 CFR 73.21. The applicant should portion mark text in the response to request for additional information (RAI) as appropriate to identify SGI (or Official-Use-Only Security-Related Information) that reveals the specific details of physical protection.

ANSWER:

Safeguards Contingency Plan, Section 8, Protective Strategy 3rd paragraph, 2nd to last sentence, Page C-25, pertains to an engineered feature in the Owner Controlled Area and not the security access point for CPNPP Units 3 and 4. Therefore, this system is not an engineered system for CPNPP Units 3 and 4 and there are no interface requirements between CPNPP Units 3 and 4 and CPNPP Units 1 and 2. *A Memorandum of Understanding (MOU) will be in place to transmit information regarding the Owner Controlled Area and SAP in the Owner Controlled Area from CPNPP Units 1 and 2 to CPNPP Units 3 and 4.* See the response to Question 10.06.01-47 below. *The PSP will be revised to address the MOU.*

Impact on R-COLA

The PSP will be revised in the next COLA revision.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-47

47. **(U)** Part 8, Safeguards Contingency Plan, Section 8, Protective Strategy (1st paragraph, 2nd line, Page C-26): Include CPNNP Unit 4 in "the Memorandum of Understanding (MOU) will be in place prior to operations on CPNPP Unit 3 to address this arrangement."

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for combined license (COL) include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT and maintain at all time such capabilities. The reliance on Units 1 and 2 to support and response to security events in the OCA that is shared between the plants include both CPNPP Units 3 and 4. The plans for an MOU should include CPNPP Unit 4.

ANSWER:

The Safeguards Contingency Plan will be revised to state that a MOU will be in place to transmit information regarding Owner-Controlled Area patrols from CPNPP Units 1 and 2 to CPNPP Units 3 and 4.

Impact on R-COLA

The Safeguards Contingency Plan will be revised in the next COLA revision.

Impact on S-COLA

None.

Impact on DCD

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-48

48. **(U)** Part 8, Safeguards Contingency Plan, Section 8, Protective Strategy (2nd paragraph, 2nd line, Page C-26): Verify, and indicate, the design dimensions of the concrete blocks indicated in this section and the dimensions indicated in Sections 11.2.1 and 11.2.2 of the PSP. Specifically, verify whether that the thickness indicated is correct and indicate the length for the blocks described in this section.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for combined license (COL) include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT and maintain at all time such capabilities. Title 10 CFR 52.6, Completeness and accuracy of information, requires information provided "shall be complete and accurate in all material respects." The design dimensions for concrete blocks providing the same physical protection functions are inconsistent between security plans.

(U) Note: The information addressing specific details related to security features or providing security functions will be safeguards information (SGI) and should be marked and protected in accordance with 10 CFR 73.21. The applicant should portion mark text in the response to request for additional information (RAI) as appropriate to identify SGI (or Official-Use-Only Security-Related Information) that reveals the specific details of physical protection.

ANSWER:

The descriptions of the concrete blocks contained in PSP Sections 11.2.1 and 11.2.2, are consistent with the description contained in the Safeguards Contingency Plan, page C-26. The PSP descriptions refer to multiple layers of a specific thickness. The Safeguards Contingency plan refers to the composite thickness of the multiple layers of concrete blocks.

Impact on R-COLA

None.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-49

49. **(U)** Part 8, Safeguards Contingency Plan, Section 8, Protective Strategy (Page C-24 through C-27): Indicate reference to MHI Technical Report UAP-SGI-080002 for descriptions of design and performance requirements of physical protection systems and supporting technical bases and assumptions for the summary of protective strategy described in this section.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for COL include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT and maintain at all time such capabilities. The descriptions and details for design, performance requirements, and technical assumptions for the summary for detection, assessment, communications, delay and response of the protective strategy, including integration of programmatic requirements for IMP, in Section 8 of the SCP are described in the MHI Technical Report UAP-SGI-080002, Revision 1, dated January 22, 2010 (i.e., Sections 5 and 6, attachments, and Appendix A, "Example Protective Strategy for US-APWR Reference Plant"), and should be incorporated by reference.

ANSWER:

See the response to Question 13.06.01-1, which states that the High Assurance Evaluation Assessment, including Appendix A, is described in FSAR Section 13.6.

Impact on R-COLA

None.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-50

50. **(U)** Part 8, Safeguards Contingency Plan, Section 8, Protective Strategy (3rd line, Page C-27): Provide clarification and assumptions for what is considered the "soft walls." Identify their locations and describe the design and constructions requirements for categorizing the exterior structural walls of the power block buildings as "soft walls." In addition, clarify whether other portions of the exterior perimeter walls of the power block (vital island and buildings) are provided with the same protection to neutralize adversaries attempting to access the vital areas by other than the normal entrances and exits and soft walls.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for combined license (COL) include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT and maintain at all time such capabilities. Title 10 CFR 73.55(b)(ii) requires defense-in-depth for physical protection program. Defense-in-depth is required to provide assurance of layered protection to neutralize adversaries. Clarification is needed to understand the technical basis and assumptions for the describe protection of power block against the DBT adversaries.

(U) Note: The information addressing specific details related to security features or providing security functions will be safeguards information (SGI) and should be marked and protected in accordance with 10 CFR 73.21. The applicant should portion mark text in the response to request for additional information (RAI) as appropriate to identify SGI (or Official-Use-Only Security-Related Information) that reveals the specific details of physical protection.

ANSWER:

The term "soft walls" is used to describe walls other than steel-reinforced concrete walls. For buildings within the power block, soft walls are limited to the exterior walls of the turbine building. The exterior walls of the turbine building are constructed of steel framework with steel wall covering such as sheet metal. The turbine building exterior walls are categorized as soft walls because they are considered to be more

easily breached than that of a thick steel reinforced concrete wall. The turbine building is not a vital area. Other buildings not within the power block, such as the interim radwaste storage facility, may utilize a soft wall structure as well.

The exterior walls of the power block, including the turbine building, have overlapping fields of fire from the external BBREs. This will ensure that adversaries attempting to access the vital areas by other than the normal entrances and exits and soft walls will be identified and neutralized.

Safeguards Contingency Plan, Section 8, Protective Strategy (3rd line, Page C-27), will be revised to state "...with overlapping fields of fire that protect the exterior walls of the power block."

Impact on R-COLA

The Safeguards Contingency Plan will be revised in the next COLA revision.

Impact on S-COLA

None.

Impact on DCD

None.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

Comanche Peak, Units 3 and 4

Luminant Generation Company LLC

Docket Nos. 52-034 and 52-035

RAI NO.: 4585 (CP RAI #161)

SRP SECTION: 13.06.01 - Physical Security - Combined License

QUESTIONS for Reactor Security Rulemaking and Licensing Branch (NSIR/DSP/RSRLB)

DATE OF RAI ISSUE: 4/30/2010

QUESTION NO.: 13.06.01-51

51. **(U)** Part 8, Safeguards Contingency Plan, Section 8, Protective Strategy (2nd sentence, 2nd paragraph, Page C-27): Provide clarification and the design and performance requirements for the planned camera systems as indicated. Include in the RAI response the following: (a) the intended application of the camera system for the assessment; (b) describe, in general, the types of technology that may be applied to meet both functions stated; (c) describe the differences between the camera systems described in this section and Section 15.2 of the PSP; (d) describe the design considerations for interface of the camera systems with the CAS and SAS, if any; and (f) describe the design and performance requirements for secondary power supply for assuring systems availability in the event of loss of primary power.

(U) Regulatory Basis: Subpart C of Title 10 CFR (10 CFR) 52, § 52.79(a)(35)(i) and (ii) requires that information submitted for combined license (COL) include how the applicant will meet the requirements of 10 CFR 73 and descriptions of implementation of the physical security plan. Title 10 CFR 73.55(b)(3)(i) requires applicant to ensure that the capabilities to detect, assess, interdict, and neutralize the DBT and maintain at all time such capabilities. The design of physical protection systems beyond the scope of the DC is required as COL Information Item 13.6.1. Title 10 CFR 52.80(a) required the application to contain information for ITA and criteria necessary and sufficient to provide reasonable assurance that the facility has been constructed and will operate in conformity with the combined license, the provisions of the Act, and the Commission's rules and regulations. The applicant describes a physical protection system that may be applied for performing detection, assessment, and aid in neutralization of adversaries. Additional descriptions of design and performance requirements are needed to understand capabilities and intended functions to establish the design basis for licensing and sufficient details of design and criteria for verification by inspections, tests, and/or analyses. The descriptions may conform to guidelines of Regulatory Guide 1.206 to meet the requirement of 10 CFR 52.80(a).

(U) Note: The information addressing specific details related to security features or providing security functions will be safeguards information (SGI) and should be marked and protected in accordance with 10 CFR 73.21. The applicant should portion mark text in the response to request for additional information (RAI) as appropriate to identify SGI (or Official-Use-Only Security-Related Information) that reveals the specific details of physical protection.

ANSWER:

(a - f) The BREs will not have camera capability. Section 8 of the PSP will be revised to delete the second sentence of the second paragraph on page C-27.

Impact on R-COLA

The PSP will be revised in the next COLA revision.

Impact on S-COLA

None.

Impact on DCD

None.

Attachment 2

Marked-up FSAR Revision 1 Pages (Public Version)

[FSAR Revision 1 pages 13.1-3, 13.1-4, 13.4-7, 13.4-8, 13.6-1, 13.6-2, 13.6-3, 13.6-4, and 13.6-5]

Nuclear Officer is assisted by the Site Vice President, the Vice President, Nuclear Engineering and Support, and the Director, Oversight and Regulatory Affairs.

13.1.1.2.1 CPNPP Units 3 and 4 Site Organization

The CPNPP Units 3 and 4 Site Organization is shown in Figure 13.1-203. The CPNPP Units 3 and 4 operating organization, which reports directly to the Site Vice President, is discussed in Subsection 13.1.2. Operational support organizations such as Plant Support Nuclear and Nuclear Training, as well as Maintenance, Radiation Protection, Work Control/Outages, and Industrial Safety, are also described in Subsection 13.1.2.

- Site Vice President - The Site Vice President reports directly to the Executive Vice President and Chief Nuclear Officer, and is responsible for directing the operation and maintenance of CPNPP Units 3 and 4 in a reliable, safe and economic manner, in compliance with federal, state, and local laws, regulations, licenses and codes, and within established corporate and Nuclear Generation policies, plans, and procedures for implementing the appropriate portions of the Nuclear Policy Statements. The Site Vice President is assisted by the Plant Manager, the Nuclear Training Manager, the Director, Performance Improvement, and the Manager, Plant Support Nuclear (which includes Emergency Preparedness, Security, and Environmental).
- Director, Performance Improvement - The Director, Performance Improvement reports directly to the Site Vice President, and is responsible for trending and analysis of conditions adverse to quality, review and assessment of nuclear industry operating experience impact on CPNPP Units 3 and 4, administering and facilitating the Corrective Action Program, identifying and evaluating significant trends in human performance, and administering and facilitating the Human Performance, Self Assessment and Benchmarking Programs. The Director, Performance Improvement is assisted by the Manager, Corrective Action Program.
- Review Committees - Independent reviews of activities affecting plant safety and safety/security interface during the operations phase are performed by the Operations Review Committee (ORC) and the Station Operations Review Committee (SORC). The ORC is the designated corporate level review committee that provides independent review of CPNPP activities. The SORC is a CPNPP Units 3 and 4 site management standing committee that functions as an onsite operating organization review committee. The ORC reports directly to the Executive Vice President and Chief Nuclear Officer. The ORC immediately advises the Executive Vice President and Chief Nuclear Officer on all matters adversely affecting nuclear safety. The SORC provides a similar, site-level function and reports directly to the Plant Manager. RCOL2_13.06.01-3
- Programmatic Controls - Work planning and controls, corrective action and reporting programs, etc. are established to assess and manage potential safety and security issues to ensure that emergent and planned operations or activities are identified, reviewed, approved, monitored and RCOL2_13.06.01-18

documented as appropriate. These programmatic controls include reviews of proposed changes to the facility as described in the FSAR; reviews of violations, deviations and reportable events; results of investigations; review of corrective actions; and review of audits to ensure that safety issues and issues involving physical protection, including safety/security interface, will be appropriately addressed. RCOL2_13.06.01-18

Multiple layers of protection are provided to preserve unit integrity, including Organizational attributes and controls. Organizationally, operators and other shift members are assigned to a specific unit. Physical separation of units helps to minimize wrong-unit activities. In addition, station procedures and programs provide operating staff with methods to minimize human error including tagging programs, procedure adherence requirements, and training. As well as the ongoing protection it affords to existing CPNPP Units 1 and 2, the implementation of this protection strategy also applies to preserving the integrity between the existing CPNPP Units 1 and 2 and the new CPNPP Units 3 and 4.

Licensed Operators will license on both CPNPP Units 3 & 4 and other shift personnel will receive training on both units. This will allow the flexibility to rotate personnel between units on an as-needed basis.

13.1.1.2.2 Nuclear Engineering and Support Organization

The CPNPP Units 3 and 4 Support Organization is shown in Figure 13.1-204. The Support organization reports directly to the Vice President, Nuclear Engineering and Support. Support organizations include Site Engineering and Engineering Support.

- Vice President, Nuclear Engineering and Support - The Vice President, Nuclear Engineering and Support reports directly to the Executive Vice President and Chief Nuclear Officer, and is responsible for performing design and engineering activities; providing technical support to other Nuclear Generation functions; developing and maintaining an integrated administrative services program which includes Document Control and Records Management; providing and coordinating regulatory rate case support; and implementing the appropriate portions of the Nuclear Policy Statements. In addition, the Vice President, Nuclear Engineering and Support, is responsible for development of new nuclear generation, (which is referred to as the "NuBuild Project"). The Vice President, Nuclear Engineering and Support is assisted by the Director, Site Engineering, the Director, Engineering Support, the Director, NuBuild Project, and the Manager, NuBuild Quality Assurance.

- Director, Engineering Support - The Director, Engineering Support reports directly to the Vice President, Nuclear Engineering and Support and is responsible for providing for the development and implementation of specific major scope plant modifications and/or engineering projects including interface with involved off-site vendor organizations, evaluations

STD COL 13.4(1)

Table 13.4-201 (Sheet 6 of 9)

Operational Programs Required by NRC Regulation and Program Implementation

Item	Program Title	Program Source (Required By)	FSAR (SRP) Section	Implementation		
				Milestone	Requirement	
14.	Emergency Planning	10 CFR 50.47 10 CFR 50, Appendix E	13.3	Full participation exercise conducted within 2 years of scheduled date for initial loading of fuel.	10 CFR 50, Appendix E.IV.F.2a(ii)	
				Onsite exercise conducted within 1 year before the schedule date for initial loading of fuel.	10 CFR 50, Appendix E.IV.F.2a(ii)	
				Detailed implementing procedures for emergency planning submitted no less than within 180 days prior to scheduled date for initial loading of fuel.	10 CFR 50, Appendix E.V.	
15.	Security Program	10 CFR 50.34(c)				
	• Cyber Security Program	10 CFR 73.54	13.6	Prior to receipt of fuel on-site for Units 3 and 4 (in the protected area)	License Condition	RCOL2_13.06.01-4
	• Physical Security Program	10 CFR 73.55 10 CFR 73.56 10 CFR 73.57 10 CFR 26	13.6	Prior to receipt of fuel on-site for Units 3 and 4 (in the protected area)	License Condition	RCOL2_13.06.01-4
	• Safeguards Contingency Program	10 CFR 50.34(d) 10 CFR 73, Appendix C	13.6	Prior to receipt of fuel on-site for Units 3 and 4 (in the protected area)	License Condition	RCOL2_13.06.01-4

STD COL 13.4(1)

Table 13.4-201 (Sheet 7 of 9)

Operational Programs Required by NRC Regulation and Program Implementation

Item	Program Title	Program Source (Required By)	FSAR (SRP) Section	Implementation		
				Milestone	Requirement	
	• Training and Qualification Program	10 CFR 73, Appendix B	13.6	Prior to receipt of fuel on-site for Units 3 and 4 (in the protected area)	License Condition	RCOL2_13.06.01-4
16.	Quality Assurance Program Operation	10 CFR 50.54(a) 10 CFR 50, Appendix A (GDC 1) 10 CFR 50, Appendix B	17.5	30 days prior to scheduled date for the initial loading of fuel	10 CFR 50.54(a)(1)	
17.	Maintenance Rule	10 CFR 50.65	17.6	Prior to fuel load authorization per 10 CFR 52.103(g)	10 CFR 50.65(a)(1)	
18.	Motor-Operated Valve Testing	10 CFR 50.55a(b)(3)(ii)	3.9.6	Prior to Initial fuel load	License Condition	
19.	Initial Test Program	10 CFR 50.34 10 CFR 52.79(a)(28)	14.2	Prior to the first construction test for the Construction Test Program Prior to the first preoperational test for the Preoperational Test Program Prior to Initial fuel loading for the Startup Test Program	License Condition	
20.	Fitness for Duty Program	10 CFR ~~Part~~ 26				RCOL2_NONE-2
	~~Construction Mgt & Oversight personnel~~	~~10 CFR Part 26 A-H, N and O~~	~~13.7~~	~~Prior to on-site construction of safety or security related SSCs.~~	~~License Condition~~	
	~~Construction Workers & First Line Supv.~~	~~10 CFR 26 Subpart K~~	~~13.7~~	~~Prior to on-site construction of safety or security related SCCs.~~	~~License Condition~~	

13.6 SECURITY

This section of the referenced DCD is incorporated by reference with the following departures and/or supplements.

STD COL 13.6(1) 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, the safeguards contingency plan. The Security Plan (provided in CPNPP Units 3 and 4 Combined License Application Part 8) and Cyber Security Plan are submitted to the NRC ~~as separate licensing documents~~ 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. RCOL2_13.06.01-1 RCOL2_13.06.01-7

CP COL 13.6(2) **13.6.1 Physical Security – Combined License**

Replace the content of DCD Subsection 13.6.1 with the following:

As stated above, the Security Plan and the Cyber Security Plan are submitted to the NRC ~~as separate licensing documents~~ to fulfill the requirements of 10 CFR 52.79(a)(35) and 10 CFR 52.79(a)(36). The site specific physical security features and capabilities that are beyond the scope of the certified standard plant design are described in the CPNPP Units 3 and 4 physical security plan (PSP) (Ref. 13.06-201), Appendix A of the High Assurance Evaluation Assessment (Ref. 13.06-7) and in Section 13.6.2 below. RCOL2_13.06.01-7 RCOL2_13.06.01-6

CP COL 13.6(2) **13.6.2 US-APWR Physical Security** RCOL2_13.06.01-1

Replace the second paragraph of DCD Subsection 13.6.2 with the following two paragraphs:

(SRI)

RCOL2_13.06.01-1

(SRI)

CP COL 13.6(2) **13.6.2.1 Barriers, Isolation Zone, and Controlled Access Points**

Replace the content of DCD Subsection 13.6.2.1 with the following:

RCOL2_13.06.01-8

(SRI)

[ ] (SRI)

13.6.2.2 Vital Areas and Vital Equipment

CP COL 13.6(3) ~~Delete the last sentence of the first paragraph in DCD Subsection 13.6.2.2.~~ Replace the last sentence of the first paragraph in DCD Subsection 13.6.2.2 with the following: RCOL2_13.06.01-1

CP COL 13.6(4) [ ] (SRI)

Replace the last paragraph in DCD Subsection 13.6.2.2 with the following:

[ ] (SRI)

CP COL 13.6(2) **13.6.2.3 Alarm Systems and Detection Aids**

Replace the second paragraph in DCD Subsection 13.6.2.3 with the following:

[-] RCOL2_13.06.01-10 (SRI)

CP COL 13.6(2) **13.6.2.4 Security Lighting**

Replace the content of DCD Subsection 13.6.2.4 with the following:

[ ] RCOL2_13.06.01-11 (SRI)

CP COL 13.6(5) **13.6.2.5 Security Communication Systems**

Delete the last sentence of the first paragraph in DCD Subsection 13.6.2.5.

Replace the last sentence of the last paragraph in DCD Subsection 13.6.2.5 with the following:

[ ] RCOL2_13.06.01-8 (SRI)

CP COL 13.6(2) **13.6.2.6 Security Power**

Delete the last paragraph in DCD Subsection 13.6.2.6.

13.6.4 Combined License Information

Replace the content of DCD Subsection 13.6.4 with the following.

STD COL 13.6(1) ***13.6(1)*** *The plant overall security plan and implementation schedule*
This COL item is addressed in Section 13.6, Table 13.4-201 and Section 3 of Part 10. RCOL2_13.06.01-12

CP COL 13.6(2) ***13.6(2)*** *Site specific security features and capabilities.*
This COL item is addressed in Section 13.6.1, 13.6.2.1, 13.6.2.3, 13.6.2.4 and 13.6.2.6. ~~and the physical security plan.~~ RCOL2_13.06.01-12

CP COL 13.6(3) ***13.6(3)*** Identification of Vital Equipment by Subsequent COL Applicants.
To the extent applicable, this COL item is addressed in Section 13.6.2.2.

CP COL 13.6(4) ***13.6(4)*** *Provision of the secondary alarm station by single unit sites.*
To the extent applicable, this COL item is addressed in Section 13.6.2.2.

CP COL 13.6(5) ***13.6(5)*** *Communication capability with local law enforcement agencies.*
This COL item is addressed in Section 13.6.2.5.~~ and the physical security plan.~~ RCOL2_13.06.01-12

13.6.5 References

Add the following reference after the last reference in DCD Subsection 13.6.5.

13.6-201 Comanche Peak Nuclear Power Plant - Units 3 and 4 Security Plan, Training and Qualification Plan, Safeguards Contigency Plan, Revision 1, 2009.