Nuclear Innovation
North America LLC
122 West Way, Suite 405
Lake Jackson, Texas 77566
979-316-3000

September 17, 2014
U7-C-NINA-NRC-140028

U. S. Nuclear Regulatory Commission
Attention: Document Control Desk
One White Flint North
11555 Rockville Pike
Rockville, MD 20852-2738

South Texas Project
Units 3 and 4
Docket Nos. 52-012 and 52-013
Response to Request for Additional Information

Attached is the Nuclear Innovation North America, LLC (NINA) response to an NRC staff question in Request for Additional Information (RAI) letter 448 related to SRP Section 1.5. The attachment to this letter contains the response to the following RAI question:

01.05-37

There are no commitments in this submittal.

If you have any questions, please contact me at (979) 316-3011 or Bill Mookhoek at (979) 316-3014.

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

Executed on 9/17/14

Scott Head
Manager, Regulatory Affairs
NINA STP Units 3&4

Attachment:

RAI 01.05-37

D091
NRO

Cc: w/o attachment except*
(paper copy)

Director, Office of New Reactors
U. S. Nuclear Regulatory Commission
One White Flint North
11555 Rockville Pike
Rockville, MD 20852-2738

Regional Administrator, Region IV
U. S. Nuclear Regulatory Commission
1600 E. Lamar Blvd.
Arlington, Texas 76011-8064

Kathy C. Perkins, RN, MBA
Assistant Commissioner
Division for Regulatory Services
Texas Department of State Health Services
P. O. Box 149347
Austin, Texas 78714-9347

Robert Free
Radiation Inspections Branch Manager
Texas Department of State Health Services
P. O. Box 149347
Austin, Texas 78714-9347

*Steven P. Frantz, Esquire
A. H. Gutterman, Esquire
Morgan, Lewis & Bockius LLP
1111 Pennsylvania Ave. NW
Washington D.C. 20004

*Tom Tai
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852

(electronic copy)

*Tom Tai
Fred Brown
U. S. Nuclear Regulatory Commission

Jamey Seeley
Nuclear Innovation North America

Peter G. Nemeth
Crain, Caton and James, P.C.

Richard Peña
Kevin Pollo
L. D. Blaylock
CPS Energy

QUESTIONS

01.05-37

Regulatory Basis:

The provisions of 10 CFR 73.55(b)(4), require, in part, that:

(1) The licensee shall establish and maintain a physical protection program, to include a security organization, which will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.

(2) To satisfy the general performance objective of paragraph (b)(1) of this section, the physical protection program must protect against the design basis threat of radiological sabotage as stated in § 73.1.

(3) The physical protection program must be designed to prevent significant core damage and spent fuel sabotage. Specifically, the program must:
   (i) Ensure that the capabilities to detect, assess, interdict, and neutralize threats up to and including the design basis threat of radiological sabotage as stated in § 73.1, are maintained at all times.
   (ii) Provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure the effectiveness of the physical protection program.

(4) The licensee shall analyze and identify site-specific conditions, including target sets, that may affect the specific measures needed to implement the requirements of this section and shall account for these conditions in the design of the physical protection program.

The provisions of 10 CFR 50.54(p)(1) require, in part, that, "The licensee shall prepare and maintain safeguards contingency plan procedures in accordance with appendix C of part 73 of this chapter for affecting the actions and decisions contained in the Responsibility Matrix of the safeguards contingency plan. The licensee may not make a change which would decrease the effectiveness of a physical security plan, or guard training and qualification plan, or cyber security plan prepared under § 50.34(c) or § 52.79(a), or part 73 of this chapter, or of the first four categories of information (Background, Generic Planning Base, Licensee Planning Base, Responsibility Matrix) contained in a licensee safeguards contingency plan prepared under § 50.34(d) or § 52.79(a), or part 73 of this chapter, as applicable, without prior approval of the Commission. A licensee desiring to make such a change shall submit an application for amendment to the licensee's license under § 50.90.

The provisions of 10 CFR 50.54(p)(2) require, in part, that, "The licensee may make changes to the plans referenced in paragraph (p)(1) of this section, without prior Commission approval if the changes do not decrease the safeguards effectiveness of the plan. The licensee shall maintain records of changes to the plans made without prior Commission approval for a period of 3 years

from the date of the change, and shall submit, as specified in § 50.4 or § 52.3 of this chapter, a report containing a description of each change within 2 months after the change is made. Prior to the safeguards contingency plan being put into effect, the licensee shall have:

(i) All safeguards capabilities specified in the safeguards contingency plan available and functional;

(ii) Detailed procedures developed according to appendix C to part 73 of this chapter available at the licensee's site; and

(iii) All appropriate personnel trained to respond to safeguards incidents as outlined in the plan and specified in the detailed procedures."

eRAI Question

The NRC staff requests clarification pertaining to how the applicant, once licensed, will analyze and identify changes in the site-specific conditions related to the structures, systems, and components (SSCs) (described in certain technical reports), resulting from changes made to the STP Units 3 and 4 between issuance of the COL and the security program implementation milestones provided in the FSAR to ensure that the security plan continues to meet 10 CFR 73.55(b)(4). Also, clarify how the applicant, once licensed, will ensure that the as-built plant continues to meet all physical protection program design and performance criteria in 10 CFR 73.55 at the time the physical protection program is implemented.

The applicant's response should:

a. Describe how all changes of SSCs and related design information are reviewed for any impact on the physical protection program.

b. Describe how the physical protection program, to include the security plans (consisting of the physical security plan, training and qualification plan, safeguards contingency plan, and cyber security plan), will be revised to address changes that affect (both beneficial and adverse) the protective strategy with the as-built configuration.

Question:

a. Describe how all changes of SSCs and related design information are reviewed for any impact on the physical protection program.

Response:

Changes to SSCs and related design information are reviewed for any impact on the physical protection program during the period between the issuance of the COL and the security program implementation milestones provided in FSAR Table 13.4S-1.

Before a change is implemented into the site design an initial impact review is performed by the Engineering, Procurement, and Construction (EPC) team as part of the overall configuration management process. This is a cross-disciplinary review by the EPC team that includes identification of any security impact aspects of the change. If security impact issues are noted, Security Subject Matter Experts are consulted to determine if additional changes are required. The need to revise security plan documentation, procedures, processes, and training is determined in this step.

The impact review of a change includes possible impacts, direct or indirect, on the Physical Security Plan, Cyber Security Plan, Safeguards Contingency Plan, the Security Personnel Training and Qualification Plan, or the overall Security Program. If a possible impact is noted, a detailed screening is performed to consider the following items:

1. SSCs, Processes, and Programs used to detect, assess, interdict or neutralize a potential radiological threat.
2. SSCs, Processes, and Programs used for the Physical Security Plan defense-in-depth capability.
3. SSCs, Processes, and Programs used to implement the Training and Qualification plan.
4. SSCs, Processes, and Programs used to implement the Safeguards Contingency Plan.
5. Safety/Security Interface Issues including:
    a) Impeding the security force response;
    b) The safety of security personnel and non-security personnel due to security features or program changes;
    c) Impeding Operations access for responding to plant emergencies;
    d) Emergency Planning activities and preplanned emergency response actions.

If a change to SSCs and related design information results in the need to revise security plan documentation, procedures, processes, or training, the required revisions will be made as described in response to question b.

Question:

b. Describe how the physical protection program, to include the security plans (consisting of the physical security plan, training and qualification plan, safeguards contingency plan, and cyber security plan), will be revised to address changes that affect (both beneficial and adverse) the protective strategy with the as-built configuration.

Response:

The process described above will aid in identification of changes that need to be made to the security plans in response to changes to the design. The security plans, which include the Physical Security Plan, Cyber Security Plan, Safeguards Contingency Plan, and the Security Personnel Training and Qualification Plan will be updated, as required. Changes to security procedures will be updated using the processes described in Section 13.5, "Plant Procedures" of the STP 34 FSAR. Plant changes that may impact the Security Strategy are evaluated and the Physical Security Plan and the strategy are updated with the results of the evaluation prior to the implementation of the Security Program.

Based on the results of the screening described in question a above, a 50.54(p)(1) evaluation is performed, if required. If NRC approval of the change is required, a license amendment request will be submitted. If NRC approval of a change is not required, but security plan(s) information is updated with the change, a 50.54(p)(2) report describing each change will be submitted to the NRC no later than 2 months after the change is made to the Security Plan.

An additional control maintaining as-built plant compliance with security requirements is the I Inspection, Tests, Analyses and Acceptance Criteria (ITAAC) closure and maintenance process. Physical Security ITAAC are in Part 9 of the STP 34 COLA. The adequacy of plant changes that affect the security system design and compliance with the security plans are confirmed through the ITAAC closure and maintenance process. Security ITAAC will be closed and maintained pending NRC verification supporting the 10 CFR 52.103(g) finding.

FSAR Section 13.5.3.4.1 Administrative Procedures contains a statement, which commits to having a process for implementing the safety/security interface requirements of 10 CFR 73.58. In developing the safety/security interface process for the time period from issuance of the Combined License until security program implementation, the guidance contained in Regulatory Guide (RG) 5.74, "Managing the Safety/Security Interface," will be used. As is the case for 10 CFR 73.58, this RG was generally written for operating plants and uses terminology and concepts that may not all be applicable to plants during construction. A few examples are provided below:

- The term "compensatory actions" used in 10 CFR 73.58 and RG 5.74 is understood to refer to those measures specified in the Security Plan, which is not required to be implemented until near the end of the plant construction period. Thus, if all or a portion of a security system is temporarily removed from service during a time when the Security Plan has not been implemented, the compensatory measures specified in the Security Plan would not be taken.
- If a permanent plant design change is being considered that could affect the response capabilities of the security force, such as the relocation of a door or passageway within the plant, that change would be evaluated and actions may include developing changes to the security plan. When the design change is finalized and incorporated into the design documents, then changes to the Security Plan and/or security procedures will be made.
- If a temporary condition is identified that disables an emergency response facility or feature and the Emergency Plan has not yet been implemented, then mitigative actions would not be taken.
- If a permanent plant design change is being considered that alters the capabilities of an emergency response facility, that change would be evaluated and actions may include developing changes to the Emergency Plan or Emergency Plan Implementing Procedures. When the design change is finalized and incorporated into the design documents, the change for the Emergency Plan or the Emergency Plan Implementing Procedures will be made.

With this understanding of the limits of 73.58 compliance and RG 5.74 guidance during the construction phase, text will be added to the STP 34 FSAR Chapter 13 to indicate the requirement to have a process in place for assessing the safety/security interface requirements outlined in 10 CFR 73.58 at the time of COL issuance based on the information on hand at the time of the review.

A markup of the STP 34 COLA change is included below.

COLA Part 2, FSAR Chapter 13 will be revised to add text to Section 13.5.3.4.1 Administrative Procedures item (2) second bullet shown below.

- A process for implementing the safety/security interface requirements of 10 CFR 73.58.

  A process is in effect between the time of issuance of the combined license and prior to Security Program implementation during the design and construction period to implement the safety/security interface requirements of 10 CFR 73.58 and the guidance of RG 5.74. This process is used to manage safety/security interface while the security procedures and emergency plan implementing procedures are being developed and implemented.