CCNPP3eRAIPEm Resource

From: Arora, Surinder
Sent: Tuesday, January 22, 2013 2:09 PM
To: Infanger, Paul; UNECC3Project@unistarnuclear.com
Cc: CCNPP3eRAIPEm Resource; Segala, John; Wilson, Anthony; Erlanger, Craig; Coflin, Monika; Miernicki, Michael; McLellan, Judith
Subject: Final RAI 383 NSIR 6977
Attachments: FINAL RAI 383 NSIR 6977.doc

Paul,

Attached is Final RAI No. 383 (eRAI No. 6977) pertaining to your Cyber Security submittal for the Combined License Application for CCNPP3. The draft of this RAI was issued to UniStar on January 8, 2013. A clarification phone call, requested by UniStar, was held on January 18, 2013, however, no changes to the draft questions were required by this clarification phone call. This email, therefore, transmits the "final" version of the RAI with no changes to the previously transmitted draft questions.

The schedule that we have established for review of your application assumes that your technically complete response to the RAI question or a schedule for providing the response must be received within 30 days of the final RAI. Please note that if you are providing a response schedule in lieu of the technically complete response, the staff will re-evaluate the completion schedule of the chapter based on your proposed response date.

Additionally, please make sure that your response letter includes a statement whether or not your response contains any sensitive or proprietary information.

Thanks.

SURINDER ARORA, PE
PROJECT MANAGER,
Office of New Reactors
US Nuclear Regulatory Commission

Phone: 301 415-1421
FAX: 301 415-6406
Email: Surinder.Arora@nrc.gov

Hearing Identifier: CalvertCliffs_Unit3Col_RAI
Email Number: 289

Mail Envelope Properties (B46615B367D1144982B324704E3BCEEDD495448047)

Subject: Final RAI 383 NSIR 6977
Sent Date: 1/22/2013 2:08:35 PM
Received Date: 1/22/2013 2:08:37 PM
From: Arora, Surinder

Created By: Surinder.Arora@nrc.gov

Recipients:
"CCNPP3eRAIPEm Resource" <CCNPP3eRAIPEm.Resource@nrc.gov>
Tracking Status: None
"Segala, John" <John.Segala@nrc.gov>
Tracking Status: None
"Wilson, Anthony" <Anthony.Wilson@nrc.gov>
Tracking Status: None
"Erlanger, Craig" <Craig.Erlanger@nrc.gov>
Tracking Status: None
"Coflin, Monika" <Monika.Coflin@nrc.gov>
Tracking Status: None
"Miernicki, Michael" <Michael.Miernicki@nrc.gov>
Tracking Status: None
"McLellan, Judith" <Judith.McLellan@nrc.gov>
Tracking Status: None
"Infanger, Paul" <paul.infanger@unistarnuclear.com>
Tracking Status: None
"UNECC3Project@unistarnuclear.com" <UNECC3Project@unistarnuclear.com>
Tracking Status: None

Post Office: HQCLSTR01.nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	1341	1/22/2013 2:08:37 PM
FINAL RAI 383 NSIR 6977.doc	42490	

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

Request for Additional Information 383 (eRAI 6977)

Issue Date: 1/22/2013
Application Title: Calvert Cliffs Unit 3 - Docket Number 52-016
Operating Company: UniStar
Docket No. 52-016
Review Section: 13.06.06 - Cyber Security (Future SRP Section)
Application Section:

QUESTIONS

13.06.06-5

NRC requests that the word “sufficient” be removed from footnote 1 on page 10 of the Calvert Cliffs Unit 3 Cyber Security Plan. The process for handling the applicant’s concern about technical controls not being implemented is already addressed in Section 1.3.1.6, “Application of Security Controls” of the Calvert Cliffs Unit 3 Cyber Security Plan, which states, in part:

“With respect to technical security controls, {Calvert Cliffs 3 Nuclear Project, LLC} used the information collected in Section 1.3.1.4 of this plan to conduct one or more of the following for each CDA:

- Implementation of all of the security controls specified in Section 2 of this plan

- For a security control that could not be applied, implementation of alternative controls that eliminate threat/attack vectors associated with one or more of the security controls enumerated in Section 2 of this plan by:
  - Documenting the basis for employing alternative countermeasures
  - Performing and documenting an attack vector and attack tree analysis of the CDA and alternative controls to confirm that the countermeasures provide the same or greater protection as the corresponding security control identified in Section 2 of this plan
  - Ensuring that the alternative controls provide at least the same degree of protection as the corresponding security control identified in Section 2 of this plan

- Not implementing one or more of the security controls enumerated in Section 2 of this plan by:
  - Performing an attack vector and attack tree analyses of the specific security controls for the CDA that will not be implemented
  - Documenting that the attack vector does not exist (i.e., is not applicable), thereby demonstrating that those specific security controls are not necessary

{Calvert Cliffs 3 Nuclear Project, LLC} did not apply a security control when it was determined that the control would adversely impact SSEP functions. When a security control was determined to have an adverse effect, then alternate controls were used to mitigate the lack of the security control for the CDA in accordance with the process described above.”

Therefore, the footnote is not necessary as it may cause confusion during inspections.

13.06.06-6

NRC requests that the words “as applicable” be removed footnotes 3, 5, 6, 7, 8, 9, 10. 11, 12, 13, 15, and 17, which are contained throughout the Calvert Cliffs Unit 3 Cyber Security Plan. The process for handling the applicant’s concern about two conflicting cyber security controls for a certain CDA is already addressed in Section 1.3.1.6, “Application of Security Controls” of the Calvert Cliffs Unit 3 Cyber Security Plan, which states, in part:

“With respect to technical security controls, {Calvert Cliffs 3 Nuclear Project, LLC} used the information collected in Section 1.3.1.4 of this plan to conduct one or more of the following for each CDA:

- Implementation of all of the security controls specified in Section 2 of this plan

- For a security control that could not be applied, implementation of alternative controls that eliminate threat/attack vectors associated with one or more of the security controls enumerated in Section 2 of this plan by:
  - Documenting the basis for employing alternative countermeasures
  - Performing and documenting an attack vector and attack tree analysis of the CDA and alternative controls to confirm that the countermeasures provide the same or greater protection as the corresponding security control identified in Section 2 of this plan
  - Ensuring that the alternative controls provide at least the same degree of protection as the corresponding security control identified in Section 2 of this plan

- Not implementing one or more of the security controls enumerated in Section 2 of this plan by:
  - Performing an attack vector and attack tree analyses of the specific security controls for the CDA that will not be implemented
  - Documenting that the attack vector does not exist (i.e., is not applicable), thereby demonstrating that those specific security controls are not necessary

{Calvert Cliffs 3 Nuclear Project, LLC} did not apply a security control when it was determined that the control would adversely impact SSEP functions. When a security control was determined to have an adverse effect, then alternate controls were used to mitigate the lack of the security control for the CDA in accordance with the process described above.”

Therefore, footnotes 3, 5, 6, 7, 8, 9, 10. 11, 12, 13, 15, and 17 are not necessary as they may cause confusion during inspections.