PMSTPCOL PEmails

From: Anand, Raj
Sent: Thursday, January 28, 2010 1:22 PM
To: Puleo, Frederick; Mookhoek, William
Cc: Wunder, George; Tonacci, Mark; STPCOL
Subject: South Texas Project Units 3 & 4 Cyber Security RAIs
Attachments: 13.6 RAIs.doc

Hi Fred,
I am enclosing for you in draft, South Texas Projects Units 3 and 4 Cyber Security RAIs. I would like to discuss these RAIs in a conference call with you before issuance. Please let me have the date and the time for the call.
Thanks,
Raj

Raj Anand
Raj Anand
Project Manager
Division of New Reactor Licensing
Office of New Reactors
The Nuclear Regulatory Commission
E-mail: Raj.Anand@nrc.gov

Hearing Identifier: SouthTexas34Public_EX
Email Number: 2181

Mail Envelope Properties (B46615B367D1144982B324704E3BCEED2102BA31A8)

Subject: South Texas Project Units 3 & 4 Cyber Security RAIs
Sent Date: 1/28/2010 1:21:51 PM
Received Date: 1/28/2010 1:21:54 PM
From: Anand, Raj

Created By: Raj.Anand@nrc.gov

Recipients:
"Wunder, George" <George.Wunder@nrc.gov>
Tracking Status: None
"Tonacci, Mark" <Mark.Tonacci@nrc.gov>
Tracking Status: None
"STPCOL" <STP.COL@nrc.gov>
Tracking Status: None
"Puleo, Frederick" <fjpuleo@STPEGS.COM>
Tracking Status: None
"Mookhoek, William" <wemookhoek@STPEGS.COM>
Tracking Status: None

Post Office: HQCLSTR01.nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	460	1/28/2010 1:21:54 PM
13.6 RAIs.doc	59386	

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

South Texas Project Units 3 & 4 Cyber Security RAIs

1.) 10 CFR 73.54(b)(1) requires the licensee to analyze digital computer and communication systems and networks and identify those assets that must be protected against cyber attacks. Section 2.1 of the STPNOC Cyber Security Plan identifies target sets as part of the list of Critical Digital Assets (CDA). The NRC staff does not expect a list of CDAs in the cyber security plan. However the plan should describe the method for identifying CDAs. An acceptable method is in section C.3 of RG 5.71dated January 2010. Please describe the method STPNOC will use to identify CDAs.

2.) Not Used

3.) 10 CFR 73.54(b)(1) requires the licensee to analyze digital computer and communication systems and networks and identify those assets that must be protected against cyber attacks. Section 3.1.4, Identification of Critical Assets, of the STPNOC Cyber Security Plan provides a partial listing of documentation that will be developed for each critical system (CS) examined. Please explain how the following information will be documented with respect to each CS that is examined:

a. information security requirements necessary for vendors and developers to maintain the integrity of critical digital assets (CDA),
b. secure configuration, installation, and operation of the CDAs,
c. effective use and maintenance of security features/functions,
d. known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions,
e. user-accessible security features/functions and how to use those security features/functions effectively,
f. methods for user interaction with CDAs, which enables individuals to use the system in a more secure manner,
g. user responsibilities in maintaining the security of the CDA.

4.) 10 CFR 73.54(c) (2) requires licensees to apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks. Please explain how the defensive architecture does the following:

a. allocates CDAs associated with safety, important to safety and security functions, as well as support systems and equipment which, if compromised, would adversely impact safety, important to safety and security functions to Level 4 and protects them from all lower levels.
b. allows one-way data flow from Level 4 to Level 3 and from Level 3 to Level 2.
c. prohibits initiation of communications from digital assets at lower security levels to digital assets at higher security levels.
d. maintains the capability to detect, prevent, delay, mitigate, and recover from cyber attacks.

e. eliminates applications, services, and protocols not necessary to support the design-basis function of the contained critical digital assets
f. configures CSs/CDAs as described in the Security Controls section of the STPNOC cyber security plan
g. configures CSs and boundary protection systems as described in the System Hardening security controls section and the Defensive Strategy and Defense-in-Depth security controls sections.

Also, please explain how the above characteristics are consistently applied in addition to technical, management, and operational security controls.

5.) 10 CFR 73.54(c) (1) requires applicants to implement security controls to protect the digital assets within the scope of the Rule from cyber attacks. Appendix C, Section 7 of the STPNOC cyber security plan discusses defense-in-depth. How does STPNOC prevent spoofing of addresses from one security level to another?

6.) 10 CFR 73.54(c)(2) requires applicants to apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks;. Appendix C, Section 7 of the STPNOC Cyber Security Plan discusses defense-in-depth. Please explain how STPNOC imposes one way data flow control including from level 4 to level 3 and from level 3 to level 2. Does the STPNOC use hardware flow control?

7.) Not Used

8.) 10 CFR 73.54(c)(2) requires applicants to apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks.. Appendix C, Section 7 of the STPNOC Cyber Security Plan discusses defense-in-depth. Please describe whether STPNOC uses devices that enforce the security policy between each level and whether these devices detect, prevent, delay, mitigate, and recover from a cyber attack coming from the lower security level?

9.)Not Used

10.)Not Used

11.) 10 CFR 73.54(c)(1) requires applicants to implement security controls to protect the digital assets within the scope of the Rule from cyber attacks. Appendix C, Section 7 discusses defense-in-depth. Please describe bi-directional (2-way) communication between Critical Digital Assets in Level 4.

12.) 10 CFR 73.54(c) (1) requires applicants to implement security controls to protect the digital assets within the scope of 10 CFR 73.54 from cyber attacks. Appendix C, Section 7 of the STPNOC Cyber Security Plan discusses defense-in-depth. Are any non-safety system critical digital assets (CDA) that have bi-directional communication to a safety system CDA? Is the non-safety system CDA afforded the same level of protection as the safety system CDA?

13.) 10 CFR 73.54(c) (1) requires applicants to implement security controls to protect the digital assets within the scope of the Rule from cyber attacks. Appendix C, Section 7 of the STPNOC Cyber Security Plan discusses defense-in-depth. Are Critical Digital Assets that provide data acquisition functions for CDAs in Defensive Layer 4 allocated at least Defensive Level 3 protection?

14.) 10 CFR 73.54(c) (1) requires applicants to implement security controls to protect the digital assets within the scope of the Rule from cyber attacks. Appendix C, Section 8.2 of the STPNOC Cyber Security Plan states "Tests and conducts drills of the incident response capability for CDAs [critical digital assets] at an interval defined by the risk assessment..." How are the tests and drills conducted? How is the risk assessment performed?

15.) 10 CFR 73.54(c) (1) requires applicants to implement security controls to protect the digital assets within the scope of the Rule from cyber attacks. Appendix C, Section 8.4 of the STPNOC Cyber Security Plan discusses defense-in-depth. Please describe the process of incident data collection and discuss whether STPNOC documents the type of software impacted during the incidents.

16.) 10 CFR 73.54(c)(1) requires the cyber security program to implement security controls to protect the assets identified by paragraph (b)(1) of 10 CFR 73.54 from cyber attacks. Section 4.1.2, Security Impact Analysis of Changes and Environment of STPNOC Cyber Security Plan discusses implementation of cyber security controls. Please explain how and when effectiveness analysis and vulnerability assessments/scans will be conducted to verify that the security program provides high assurance that critical digital assets and critical systems are adequately protected from cyber attack, up to and including the Design Basis Threat, and that the program has closed any identified gaps.

17.) 10 CFR 73.54(d) (3) requires applicants to ensure that modifications to assets within the scope of the Rule, are evaluated before implementation. 10 CFR 73.54(1) requires applicants to develop and maintain written policies and implementing procedures to implement the cyber security plan. 10 CFR 73.54 (g) requires applicants to review the cyber security program as a component of the physical security program in accordance with the requirements of §73.55(m), including the periodicity requirements. Section 4.1 .1, “Configuration Management,” of the STPNOC Cyber Security Plan briefly discusses the configuration management. Please explain the process used to evaluate each Critical Digital Asset modification.

18.) 10 CFR 73.54(c) (1) requires applicants to implement security controls to protect the digital assets within the scope of the Rule from cyber attacks. Several of the controls refer to a "risk assessment." The following is a list of some of the sections in the Cyber Security Plan where this term is used:

Appendix B -1.17
Appendix B -2.2
Appendix B -2.5

Appendix B -2.8
Appendix B -2.9
Appendix B -4. 3

Please explain how this/these risk assessment(s) is/are performed and how the results are used.

19.) 10 CFR 73.54(c) (1) requires applicants to implement security controls to protect the digital assets within the scope of the Rule from cyber attacks. Some of the controls describe an action that occurs "periodically". The following is a list of some of the sections on the Cyber Security Plan where this term is used:

Appendix A -3.1.1
Appendix B -1.1
Appendix B -2.1
Appendix B -3.1
Appendix B -4.1
Appendix C -1.1
Appendix C -3.1
Appendix C -3.6
Appendix C -4.1
Appendix C -5.1
Appendix C -8.1
Appendix C -9.1
Appendix C -11.2

Please explain what this period is and how it is determined.

20.)Not used.

21.) 10 CFR 73.54(d) (3) requires applicants to ensure that modifications to assets within the scope of the Rule, are evaluated before implementation. Section 4.4.2, Cyber Security Impact Analysis of Changes and Environment, of the STPNOC Cyber Security Plan states that, "These impact analyses are performed as part of the change approval process to assess the impacts of the changes on the cyber security posture of Critical Digital Assets and systems that can affect SSEP functions." Please explain whether issues identified during these impact analyses are entered into the corrective action program for resolution.

22.) 10 CFR 73.54(c) (1) requires applicants to implement security controls to protect the digital assets within the scope of 10 CFR 73.54 from cyber attacks. Appendix B Section 1.2, “Account Management,” of the STPNOC Cyber Security Plan briefly discusses account Management. Does STPNOC restrict access rights based on job function? Are individuals' rights reviewed when job functions change to ensure that rights remain limited to the individual's current job function?

23.) 10 CFR 73.54(c) (1) requires applicants to implement security controls to protect the digital assets within the scope of the Rule from cyber attacks. Appendix B, Section 5.5, of the of the STPNOC Cyber Security Plan states “Tests received cyber security updates on a non-production system for testing and validation prior to installing on production systems when practical and ...” How is practicality determined?

24.) 10 CFR 73.54(c) (1) requires applicants to implement security controls to protect the digital assets within the scope of the Rule from cyber attacks. Appendix B, Section 1.3, Access Enforcement, of the STPNOC Cyber Security Plan discusses the title subject. How is the cyber risk assessment performed? How is the threat analysis performed? Is the Critical Digital Asset taken offline until the vulnerability is remediated?

25.) 10 CFR 73.54(c) (1) requires licensees to implement security controls to protect the digital assets within the scope of the Rule from cyber attacks. Appendix C, Section 3.5 of the STPNOC Cyber Security Plan discusses “security alerts and advisories.” Please describe STPNOC’s plans for independently evaluating and determining the need, severity, methods and time frames for implementing security directives consistent with the cyber security controls for each CDA?

26.) 10 CFR 73.54(c) (1) requires applicants to implement security controls to protect the digital assets within the scope of the Rule from cyber attacks. Appendix C, Section 11.11 discusses supply chain protection. Does STPNOC perform an analysis for each product acquisition to determine that the product provides the security requirements necessary to address the security controls?

27.) 10 CFR 73.54(c) (1) requires licensees to implement security controls to protect the digital assets within the scope of the Rule from cyber attacks. Appendix D, Section 3.2, of the STPNOC Cyber Security Plan includes the statement: “Configures CDAs security functions as a layered structure minimizing interactions between levels of the design and avoid any dependence by lower levels on the functionality or correctness of higher levels, or” Is the word “or” at the end of the bullet meant to imply that the condition is between this bullet and the last bullet, shown below, or is the condition applicable to all the bullets in Section 3.2 and the last bullet?

- Implements alternative controls and documents the justification for alternative controls/countermeasures where a CDA cannot support security function isolation and implements the following:
    - Physically restricts access to the CDA,
    - Monitors and records physical access to the CDA to timely detect and respond to intrusions,
    - Uses auditing/validation measures (e.g., security guard rounds, periodic monitoring of tamper seals) to detect unauthorized access and modifications to the CDAs,
    - Ensures that individuals who have access to the CDA are qualified, and
    - Ensures that those individuals are trustworthy and reliable per § 73.56.

28.) 10 CFR 73.54(c) (1) requires applicants to implement security controls to protect the digital assets within the scope of the Rule from cyber attacks. Appendix C, Section 3.5: of the STPNOC Cyber Security Plan states "Implements and documents any required mitigation measures in accordance with the configuration management process." Please describe in detail the configuration management process.

29.) 10 CFR 73.54(c) (1) requires applicants to implement security controls to protect the digital assets within the scope of the Rule from cyber attacks. Appendix C, Section 6 Defensive Strategy states, "The elements of the defensive strategy are incorporated into CDAs based on the Cyber Security Baseline Assessment." Please describe in detail the Cyber Security Baseline Assessment.

30.) 10 CFR 73.54(c) (1) requires applicants to implement security controls to protect the digital assets within the scope of the Rule from cyber attacks. Appendix C Section 8 of the STPNOC's cyber security Plan discusses Attack Mitigation and Incident Response: Please describe how STPNOC's procedure mitigates the consequences of cyber attacks.