PRM-73-18
79FR56525

PUBLIC SUBMISSION

As of: December 09, 2014
Received: December 08, 2014
Status: Pending_Post
Tracking No. 1jy-8fxy-b0id
Comments Due: December 08, 2014
Submission Type: Web

Docket: NRC-2014-0165
Protection of Digital Computer and Communication Systems and Networks

Comment On: NRC-2014-0165-0002
Protection of Digital Computer and Communication Systems and Networks

Document: NRC-2014-0165-DRAFT-0017
Comment on FR Doc # 2014-22523

Submitter Information

Name: Bruce Thompson

General Comment

VIRGIL C. SUMMER NUCLEAR STATION (VCSNS) endorses the petition and recommends the NRC promptly initiate rulemaking to implement the changes proposed. The ongoing cyber security event notification rulemaking could provide a ready vehicle. Please see attached file titled "VCSNS Response [NRC-2014-0165]".

Attachments

VCSNS Response [NRC-2014-0165]

The September 22, 2014 Federal Register Notice (FRN) (*79 Fed. Reg. 56525*) docketed (Docket ID NRC-2014-0165) a petition for rulemaking (PRM-73-18) to amend the Nuclear Regulatory Commission's (NRC's) cyber security requirements in 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks," and requested comments by December 8, 2014.

VIRGIL C. SUMMER NUCLEAR STATION (VCSNS) endorses the petition and recommends the NRC promptly initiate rulemaking to implement the changes proposed. The ongoing cyber security event notification rulemaking could provide a ready vehicle.

VCSNS recognizes the cyber threat, and has a long history of addressing cyber security concerns. VCSNS broadly implements cyber security measures consistent with prudent business practices for digital systems and equipment. Additionally, VCSNS was directed by the Interim Compensatory Measures (ICM) Order (EA–02–026) to consider and address cyber safety and security vulnerabilities. In April 2003, the Orders (EA–03–086) and (EA–03–087) supplemented the Design Basis Threat and also contained language concerning the cyber threat. VCSNS was subsequently provided with a cyber security self-assessment methodology, the results of pilot studies, and a guidance document issued by the NEI to facilitate development of site cyber security programs.

VCSNS Unit 1 has spent five years implementing the Commission's cyber security requirements and, as discussed in the Petition, has implemented key protective measures with a specific emphasis on the protection of the most risk significant digital assets. Specifically, VCSNS implemented the following seven milestones at our operating nuclear power plant prior to December 31, 2012, providing a substantial level of protection to the installed critical digital assets:

1. Established a Cyber Security Assessment Team
2. Identified the Critical Systems and the Critical Digital Assets (CDAs)
3. Installed a deterministic one-way device between level 2 and level 3
4. Implemented the security control "Access Control for Portable and Mobile Devices"
5. Implemented observation and identification of obvious cyber related tampering to existing insider mitigation rounds
6. Identified, documented, and implemented NEI 08-09, Rev. 6, Appendix D, technical cyber security controls for CDAs that could adversely impact the design function of physical security target set equipment
7. Commenced monitoring and assessment activities for those target set CDAs whose security controls have been implemented.

VCSNS continues to implement the balance of the program, and is concerned with the ongoing and unnecessary burden associated with maintaining 1700 digital assets within the scope of the cyber security program for VCSNS Unit 1 – most having no nexus to protecting the health and safety of the public.

VCSNS Units 2 and 3, SCE&G's New Builds, have an estimated CDA population of 3000 CDAs per Unit - most having no nexus to protecting the health and safety of the public - under the current cyber security requirements in 10 CFR 73.54.

Examples of these include: non-safety related digital indicators, recorders, cameras, and transmitters. While these devices are important to the efficient operation of the plant, they are adequately protected by the existing plant controls such as physical protection, access authorization, behavioral observation program, network isolation, configuration management, and maintenance and testing.

VCSNS actual implementation costs will be a significant multiple of what was indicated by the NRC in the Regulatory Analysis for the Rule. The high cost of implementation and ongoing compliance has implications that are not strictly financial. The cost of implementing and maintaining the requirements of the rule directly competes with facility modifications that improve equipment reliability and reduce the likelihood of an initiating event. The funding required for implementing and maintaining the requirements of the Rule directly competes with funding that would be more beneficial to improving plant safety through facility modifications that improve equipment reliability. The current scope of the rule introduces significant and unwarranted costs in terms of compliance with 10 CFR 73.56. These issues would be resolved by the proposed rulemaking.

VCSNS believes the changes proposed in the petition would have an immediate reduction in unnecessary burden while continuing to provide high assurance of adequate protection from a cyber-attack. Specifically, the changes proposed in the petition would:

- Prevent radiological sabotage, consistent with the NRC's original intent, and long-standing physical protection program requirements;
- Continue to provide defense-in-depth protection for digital assets that have a nexus to radiological safety and security;
- Eliminate the unnecessary diversion of attention and resources from the protection of those assets that do have a nexus to radiological safety and security; and
- Enhance regulatory clarity and implementation efficiency.