PRM-73-18
79FR56525

PUBLIC SUBMISSION

As of: December 09, 2014
Received: December 08, 2014
Status: Pending_Post
Tracking No. 1jy-8fxw-tysk
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-0011
Comment on FR Doc # 2014-22523

Submitter Information

Name: Scott Bauer
Submitter's Representative: Steve Meyer
Organization: STARS Alliance LLC

General Comment

See STARS letter 14016 dated December 8, 2014

Attachments

STARS comments on Cyber Security PRM

STARS Alliance

www.starsalliance.com
1626 N. Litchfield Rd., Suite 230
Goodyear, AZ 85395
T : 623-209-7549

Alliance Members:
Callaway Energy Center
Comanche Peak Nuclear Power Plant
Diablo Canyon Power Plant
Palo Verde Nuclear Generating Station
Wolf Creek Generating Station

STARS-14016

December 8, 2014

Ms. Annette L. Vietti-Cook
Secretary
Attn: Rulemaking and Adjudications Staff
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Petition to Amend Cyber Security Requirements: Request for Comments (*Federal Register Vol.* 79, 56525, dated September 22, 2014 - Docket ID NRC-2014-0165)

Dear Ms. Vietti-Cook:

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.

STARS Alliance LLC (STARS) 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.

STARS Alliance stations recognize the cyber threat, and have a long history of addressing cyber security concerns. STARS Alliance stations broadly implement cyber security measures consistent with prudent business practices for digital systems and equipment. Additionally, STARS Alliance stations were 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. STARS Alliance stations were 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.

STARS Alliance stations have spent five years implementing the Commission's cyber security requirements and, as discussed in the Petition, have implemented key protective measures with a specific emphasis on the protection of the most risk significant digital assets. STARS Alliance stations continue to implement the

balance of the program, and are concerned with the ongoing and unnecessary burden associated with maintaining hundreds to thousands of digital assets within the scope of the cyber security program —many having no effect on safe shutdown of the plant and no nexus to protecting the health and safety of the public.

For example, at the Callaway and Wolf Creek plants, approximately 1,300 Critical Digital Assets are within the scope of the cyber security program. Devices such as meteorological towers and seismic instrumentation, which cannot be used to cause radiological sabotage, are consuming the finite resources available for implementing effective cyber security controls for equipment whose compromise could cause radiological sabotage. The ongoing monitoring requirements to ensure digital devices remain protected are significant, and these resources should be focused on the most important equipment, rather than spread across more devices than can be effectively monitored. Similarly, HVAC or heat trace devices that have only long term impacts on other devices should not require the same level of protection as the devices that could be used to directly cause radiological sabotage.

Comanche Peak maintains over 2,800 Critical Digital Assets within the scope of the cyber security program. Examples of these devices include non-safety related digital indicators, recorders, cameras, transmitters, and media converters. 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, network isolation, configuration management, maintenance and testing.

STARS provides varying degrees of cyber security for all digital devices as good business practice to protect company assets. The high levels of protection required by 10CFR73.54, however, should be focused on the equipment whose compromise could endanger the health and safety of the public.

Furthermore, STARS believes that a graded approach, based on device capabilities, is necessary in order to focus resources where they are needed most. A simple stand-alone device with few configuration options, that does not allow a compromise resulting in a future coordinated attack, should not require the same level of ongoing monitoring as a networked system employing a modern operating system. Such simple devices are sufficiently protected by the existing plant controls such as physical protection, device isolation, configuration management, maintenance and testing.

STARS believes the changes proposed in the petition would have an immediate positive impact on overall safety and security, while reducing unnecessary burden and accomplishing the objective of 10CFR73.54 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;
- Support grid reliability through protection of digital assets capable of causing a reactor trip;
- Continue to support having the NRC as the single regulatory authority for cyber 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.

Please contact me at 623-239-4359, or scott.bauer@starsalliance.com, if you have any questions regarding this letter.

Sincerely,

Scott Bauer
Regulatory Affairs Functional Area Manager
STARS Alliance LLC

SJM