PRM-73-18
79FR56525

9

PUBLIC SUBMISSION

As of: December 09, 2014
Received: December 08, 2014
Status: Pending_Post
Tracking No. 1jy-8fxt-os54
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-0006
Comment on FR Doc # 2014-22523

Submitter Information

Name: Paul Duke
Organization: PSEG Nuclear

General Comment

See attached file(s)

Attachments

Petition Amend Cyber Scty Reqmts LR-N14-0257

PSEG Nuclear LLC
P.O. Box 236, Hancocks Bridge, NJ 08038-0236

PSEG
Nuclear LLC

LR-N14-0257
December 08, 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.

PSEG Nuclear (PSEG) 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.

PSEG recognizes the cyber threat, and has a long history of addressing cyber security concerns. PSEG broadly implements cyber security measures consistent with prudent business practices for digital systems and equipment. Additionally, PSEG 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. PSEG was subsequently provided with a cyber-security self-assessment methodology, the results of pilot studies, and a guidance document issued by the Nuclear Energy Institute to facilitate development of site cyber security programs.

PSEG 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. PSEG continues to implement the balance of the program, and is concerned with the ongoing and unnecessary burden associated

with maintaining hundreds to thousands of digital assets within the scope of the cyber security program – most having no nexus to protecting the health and safety of the public.

Examples of components requiring protection under the current rule that do not have a nexus to radiological safety and security include:

- Numerous digital process instruments within balance of plant systems whose failure or compromise are easily addressed with existing plant procedures and do not result in a plant trip;
- Wireless control systems associated with plant cranes used for the movement of large loads;
- Digital chart recorders providing redundant indication of plant parameters; and
- Business computer systems associated with the accumulation of data required for plant access authorization.

While these assets 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.

The requirement to include in the cyber security plan many assets which are not critical to a design basis threat has far reaching impacts which provide little or no increase in nuclear safety. Examples of such impacts include procurement practices which are projected to significantly increase costs by requiring new vendor processes outside of the existing well-vetted procurement process, requirements for monitoring and assessment outside of current practices, and a failure to accept current maintenance rule analyses of components' risk significance.

Existing site physical security requirements have identified those systems and components that must be protected to prevent acts of radiological sabotage, and those that provide assurance that physical security responses can be implemented. Enhancement of cyber security protection for the digital portion of these systems and components is appropriate and will be provided for under the proposed rule-making; however, significant additional burden is associated with applying cyber security controls to protect critical digital assets (CDAs) when the postulated attack is specific to an active insider with physical CDA access. In this event, the application of cyber security controls to CDA's is not consistent with other elements of the physical protection program as cyber security controls are required for systems and equipment beyond the systems and equipment necessary to prevent radiological sabotage.

PSEG believes the changes proposed in the petition would have an immediate positive impact on overall safety and security while reducing unnecessary burden. 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.

There are no regulatory commitments contained in this letter.

If there are any questions, or if additional information is required, please contact James W. Shank at 856-339-1834.

Sincerely,

Paul R. Duke, Jr.
Manager - Licensing

cc: The Honorable Allison M. Macfarlane, Chairman, NRC
The Honorable Kristine L. Svinicki, Commissioner, NRC
The Honorable William C. Ostendorff, Commissioner, NRC
The Honorable Jeff Baran, Commissioner, NRC
The Honorable Stephen G. Burns, Commissioner, NRC
Mr. Mark A. Satorius, EDO, NRC
Mr. James T. Wiggins, NSIR, NRC
Mr. Barry C. Westreich, NSIR/CSD, NRC
Commitment Coordinator – Salem
Commitment Coordinator – Hope Creek
Commitment Coordinator – PSEG Corporate