

PUBLIC SUBMISSION

As of: December 09, 2014
Received: December 08, 2014
Status: Pending_Post
Tracking No. 1jy-8fxi-t0f8
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-0004

Comment on FR Doc # 2014-22523

Submitter Information

Name: Mark Burzynski

Submitter's Representative: Mark Burzynski

Organization: NewClear Day, Inc.

General Comment

PRM7318: Protection of Digital Computer and Communication Systems and Networks

The NEI petition for rulemaking correctly notes that the rules original scoping language was removed and replaced with new text when the cyber security provision was relocated to a new regulation during the original rulemaking, the rules original scoping language was removed and replaced with new text. The scoping language in the final rule promulgating 10 CFR 73.54(a) was added to the final rule and was not included in the proposed rule. Therefore, there was no opportunity for stakeholder comment on this aspect of the final rule. The practical effect of the new, more expansively worded scoping language relating to protection of digital assets against cyber-attack was likely not clear when the final rule was issued.

The industry has spent five years implementing the Commissions 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. The industry is continuing to implement the balance of the program. NewClear Day, Inc. 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. NEI has provided many examples of equipment within the scope of the rule that does not have any ability to impact radiological safety and security.

Clearly, industry efforts to perform additional analysis and implementation of cyber security controls on this type of equipment may delay other facility enhancements and dilute those resources that also provide cyber security protection of more critical digital assets.

NewClear Day, Inc. believes the changes proposed in the NEI 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.

Acting on the NEI petition would be consistent with the efforts to incorporate lessons learned into the cyber security regulations that were started with the NRC endorsement of NEI 13-10, Cyber Security Control Assessments.