PRM-73-18
79FR56525
13

PUBLIC SUBMISSION

As of: December 09, 2014
Received: December 08, 2014
Status: Pending_Post
Tracking No. 1jy-8fxx-iimp
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-0014
Comment on FR Doc # 2014-22523

Submitter Information

Name: Robin Ritzman
Address:
341 White Pond Drive
Akron, OH, 44302
Email: rritzman@firstenergycorp.com
Organization: FirstEnergy Nuclear Operating Company

General Comment

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 Commissions (NRCs) cyber security requirements in 10 CFR 73.54, Protection of Digital Computer and Communication Systems and Networks, and requested comments by December 8, 2014.

FirstEnergy Nuclear Operating Company (FENOC) 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.

FENOC recognizes the cyber threat, and has a long history of addressing cyber security concerns. FENOC broadly implements cyber security measures consistent with prudent business practices for digital systems and equipment. Additionally, FENOC was directed by the Interim Compensatory Measures (ICM) Order (EA02026) to consider and address cyber safety and security vulnerabilities. In April 2003, the Orders (EA03086) and (EA03087) supplemented the Design Basis Threat and also contained language concerning the cyber threat. FENOC 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.

FENOC 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. Specifically, FENOC implemented the following seven milestones at each of our nuclear power plants 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.

FENOC 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 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. Likewise, CDAs that are used in emergency preparedness applications, such as communication systems, while not necessarily protected by the same level of physical security, are typically protected through the use of redundancy and/or diversity. These assets are also typically behind locked doors and therefore protected from the general public and the elements.

FENOC 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 NRCs 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.

If there are any questions, or if additional information is required, please contact Robin Ritzman at 330-436-1484.