PRM-73-18
79FR56525

PUBLIC SUBMISSION

As of: December 09, 2014
Received: December 03, 2014
Status: Pending_Post
Tracking No. 1jy-8fuh-fqaz
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-0002
Comment on FR Doc # 2014-22523

Submitter Information

Name: John Parker
Address:
217 Evergrene Pkwy
Palm Beach Gardens, FL, 33410

General Comment

See attached file(s)

Attachments

Comments on NRC-2014-0165-0002_NEI Rulemaking Petition

Date: December 3, 2014

Commentor: John Parker, Nuclear Engineer

Subject: Comments on ID: NRC-2014-0165-0002, “Protection of Digital Computer and Communications Systems and Networks”, Petition for Rulemaking from Anthony Pietrangelo, filed on behalf of the Nuclear Energy Institute

Please consider adopting the rule change proposed by NEI in the subject position. The current cyber rule, 10 CFR 73.54(a)(1), scope is too broad, resulting in unnecessary, and often absurd, application of cyber security controls to plant digital equipment. Because no graded approach is endorsed by the NRC, a deterministic approach is used for compliance with the rule, and in the determination of required cyber security controls. This results in the application of controls, and the ongoing assessment of the controls, that contribute no added value, are costly to maintain, and reduce the effectiveness of the digital assets.

A primary example is found in the application of the rule to Emergency Preparedness (EP) communications. Telephones used for EP communications are Critical Digital Assets, under the scope of the rule. Evaluation of these assets under NEI 13-10 results in the requirement for a minimum set of cyber security controls, including Ongoing Monitoring, which includes configuration management and change control. The most conservative application of these controls has led to absurd and counter-productive requirements like:

- Telephone repairmen must be included in the security “Critical Group”.
- Telephones are treated as plant equipment subject to [10 CFR 50] App. B implementing procedures for design control and configuration control. This makes it virtually impossible, and very expensive, to maintain a telephone system.
- Telephone changes must be analyzed prior to every change, resulting in repair times of days, vs. minutes.
- Remote access for the maintenance and repair of telephones is prohibited.

Adoption of the proposed rule change would eliminate unproductive time and effort in the application of cyber security controls. Alternatives to adoption of the rule change might include: endorsement of NEI 10-09 or some other risk-informed, graded approach.