PRM-73-18
79FR56525

PUBLIC SUBMISSION

As of: December 09, 2014
Received: December 08, 2014
Status: Pending_Post
Tracking No. 1jy-8fxw-8f2a
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-0012
Comment on FR Doc # 2014-22523

Submitter Information

Name: John McCann
Address:
440 Hamilton Avenue
White Plains, NY, 10601

General Comment

See attached file(s)

Attachments

CNRO-2014-00015 - Comments on cyber security requirements

Entergy Operations, Inc.
Entergy Nuclear Operations, Inc.
440 Hamilton Avenue
White Plains, New York 10601
Tel: 914-272-3370

John F. McCann
Vice President,
Regulatory Assurance

CNRO-2014-00015

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 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.

Entergy 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.

Entergy recognizes the cyber threat, and has a long history of addressing cyber security concerns. Entergy broadly implements cyber security measures consistent with prudent business practices for digital systems and equipment. Additionally, Entergy 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. Entergy 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.

Entergy 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. Entergy 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.

The following provides an example from one of Entergy's 11 nuclear power plants pertaining to its Plant Process Computer (PPC). The PPC is a plant monitoring network, providing computer graphic displays of plant equipment configuration and parameter values such as reactor coolant system average temperature and steam generator water level. Digital or analog signals are transmitted from data acquisition instruments embedded in plant systems to digital output converters, then processed by a server and displayed on network workstations in

various locations including the control room. The PPC has a primary and backup server; however, if the PPC is not available there is no immediate automatic or Technical Specification-required impact on plant electric power output or core reactivity. The PPC does not perform any automatic digital control functions such as valve positioning, motor speed control, or control rod positioning. IP3 Safety Parameter Display System (SPDS) functionality is integrated into the design of the PPC. The SPDS display corresponds to specific sections of emergency operating procedures (EOPs) in order to complement operator use of the EOPs. However, the EOPs are constructed to allow operators to achieve timely and accurate safety status assessment either with or without the availability of the PPC. A long-term PPC outage could adversely impact the feed water system leading edge flow meter (LEFM) venturi fouling correction factor and, therefore, could result in a conservative 1-2 percent reduction in plant electric power output and a corresponding change in reactivity. For this reason the PPC is classified as important-to-safety and a Critical System (CS) within the scope of the current requirements of 10 CFR 73.54. The PPC, therefore, is placed in cyber security defense-in-depth strategy Level 3, and is accordingly deterministically isolated from lower levels by a data diode even though it is not a primary means for plant monitoring pursuant to operational decision-making.

Operations personnel are trained to validate plant parameters by control board and/or local indication prior to taking any control actions. If the PPC was infected by malware that caused incorrect indications or unavailability of PPC displays, it would rapidly become evident to plant operators, and would not present any significant risk to safe or secure plant operation, including the ability to shutdown and maintain the reactor in a safe shutdown condition, because the plant is operated by control board and local indications and controls as described above.

The PPC network includes numerous digital components, including servers, switches, routers, workstations, and printers. These components constitute over 130 CDAs. Each of these CDAs requires documentation of an assessment of the CDA as configured, against the cyber security technical controls in NEI 08-09, Revision 6, Appendix D. When broken down into actionable items, there are over 200 such controls. The result of the assessment indicates a number of actions must be implemented to satisfy the controls, including configuration of network accounts, automated network activity monitoring, and performance of periodic inspections. This represents a significant resource burden without a measurable increase in reactor and spent fuel security in both initial and ongoing activities to satisfy cyber security requirements accruing from the manner in which 10 CFR 73.54 is presently worded, although the system has no capability to cause core damage or spent fuel sabotage.

Entergy 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.

Thank you for the opportunity to provide these comments on the subject rulemaking.

Sincerely,

JFM/ghd/aye

cc: Mr. J. S. Forbes (ECH)
Mr. T. G. Mitchell (ECH)
Mr. J. A. Ventosa (HQN)
Ms. D. Jacobs (ECH)
Mr. J. A. Kowalewski (ECH)
Mr. J. F. McCann (WPO)
Mr. M. Perito (ECH)
Mr. L. Coyle (IPEC)
Mr. B. Sullivan (JAF)
Mr. J. Dent (PNPS)
Mr. K. J. Mulligan (GGNS)
Mr. M. R. Chisum (WF3)
Mr. J. G. Browning (ANO)
Mr. C. J. Wamser (VY)
Mr. E. W. Olson (RBS)
Mr. A. J. Vitale (PLP)

bcc: Mr. J. A. Clark (RBS)
Mr. J. Hardy (PAL)
Mr. E. Perkins (PIL)
Ms. S. L. Pyle (ANO)
Mr. C. Adner (JAF)
Mr. J. Nadeau (GGNS)
Mr. J. Jarrell (WF3)
Mr. R. W. Walpole (IPEC)
Mr. C. Chappell (VY)
Mr. G. H. Davant (ECH)
Mr. A. Eng (WPO)
Mr. G. Schwartz (WPO)