

# PUBLIC SUBMISSION

<b>As of:</b> December 09, 2014
<b>Received:</b> December 08, 2014
<b>Status:</b> Pending_Post
<b>Tracking No.</b> 1jy-8fxx-e551
<b>Comments Due:</b> December 08, 2014
<b>Submission Type:</b> 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-0013

Comment on FR Doc # 2014-22523

---

## Submitter Information

**Name:** Chuck Pierce

**Address:**

40 Inverness Center Parkway  
Birmingham, 35242

**Email:** cpierce@southernco.com

---

## General Comment

See attached file(s)

---

## Attachments

NL-14-1841



December 08, 2014

NL-14-1841

Ms. Annette L. Vietti-Cook  
Secretary  
Attn: Rulemaking and Adjudications Staff  
U.S. Nuclear Regulatory Commission  
Washington, DC 20555-0001

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 (*79 Fed. Reg. 56525*) docketed (Docket ID NRC-2014-0165) a petition for rulemaking (PRM-73-18) to amend the Nuclear Regulatory Commission (NRC) cyber security requirements in 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks." Comments were requested by December 8, 2014.

Southern Nuclear Operating Company (SNC) endorses the petition and recommends the NRC promptly initiate rulemaking to implement the changes proposed. The ongoing cyber security event notification rulemaking provides a ready vehicle.

SNC recognizes the cyber threat and broadly implements cyber security measures for digital systems and equipment consistent with prudent safety and business practices. Additionally, SNC was directed by the Interim Compensatory Measures Order (EA-02-026) to consider and address cyber safety and security vulnerabilities. NRC Orders (EA-03-086) and (EA-03-087) supplemented the Design Basis Threat and contained language concerning the cyber threat. Southern Nuclear Operating Company 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.

SNC has spent many years implementing cyber security measures, including the requirements ordered by the NRC. SNC has implemented key protective measures with a specific emphasis on the protection of the most risk significant digital assets. SNC continues to implement the balance of the program, and is concerned with the ongoing and unnecessary burden associated with maintaining over 8,500 components for the operating units as "Critical Digital Assets" within the cyber security program – most of which would not have the potential to impede safe shutdown of the plant if compromised.

Examples of these include: non-safety related digital indicators, recorders, smoke detectors, cameras, transmitters, and media converters. 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, network isolation, configuration

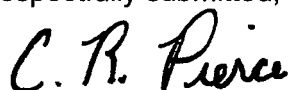
management, maintenance and testing. NRC inspectors have interpreted critical digital assets to include such things as backup valve position indicators to which an operator may refer during an abnormal plant condition. If such indicators were affected by a cyber security event, this could potentially delay an action in response to the event, but without affecting plant safety. Such an interpretation adds hundreds of components to the critical digital asset program that make no contribution to plant safety and goes well beyond any reasonable definition of "critical."

The changes proposed in the petition would facilitate a reduction in unnecessary burden while accomplishing the objective of 10CFR73.54 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 original NRC intent and long-standing physical protection program requirements;
- Continue to provide defense-in-depth protection for digital assets that have a tie to radiological safety and security;
- Eliminate the unnecessary diversion of attention and resources from the protection of those assets that have an impact on radiological safety and security; and
- Enhance regulatory clarity and implementation efficiency.

If you have any questions or comments, please contact Doug McKinney at (205) 992-5982.

Respectfully submitted,



C. R. Pierce  
Regulatory Affairs Director

CRP/dn/lac

Cc: Southern Nuclear Operating Company  
Mr. S. E. Kuczynski, Chairman, President & CEO  
Mr. D. G. Bost, Executive Vice President & Chief Nuclear Officer  
Mr. M. D. Meier, Vice President – Regulatory Affairs  
Mr. D. R. Madison, Vice President – Fleet Operations  
Mr. B. J. Adams, Vice President – Engineering  
SNC Document Services - RType: Generic CGA02.003

U.S. Nuclear Regulatory Commission  
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