Nuclear Operating Company
South Texas Project Electric Generating Station P.O. Box 289 Wadsworth, Texas 77483

December 8, 2014
NOC-AE-14003200
STI: 33993384

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 (Docket ID NRC-2014-0165) 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.

STP Nuclear Operating Company (STPNOC) 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.

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

STPNOC 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. STPNOC 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 components requiring protection under the current rule that do not have a nexus to radiological safety and security include:

- Numerous digital process instruments within balance of plant systems whose failure or compromise are easily addressed with existing plant procedures and do not result in a plant trip
- Wireless control systems associated with plant cranes used for movement large loads
- Digital Chart recorders providing redundant indication of plant parameters
- Business computer systems associated with accumulation of data reviewed to meet plant access authorization requirements
- Providing additional protection to digital components located within the current physically protected areas of the plant. The negative effects of digital compromise of the component can be easily replicated through non-digital means through routine mechanical actions such as valve operation, instrument isolation, removal of power, etc.

The impact of including plant components currently scoped into the cyber security plant are far reaching and provide little to no increase in nuclear safety. Examples include a challenging procurement process significantly increasing projected costs by having vendors perform processes outside of a well vetted procurement process that has served the industry well, on-going rule requirements for monitoring and assessment outside of current practices, a failure to accept current maintenance rule analysis of a components risk significance for exemption from additional treatment.

Site physical security requirements currently in existence have identified those systems and components that must be protected to prevent acts of radiological sabotage and those that provide assurance that physical security responses are adequately protected. Enhancement of digital components associated with these device with cyber security protection is appropriate and will be provided for with the proposed rule-making.

STPNOC 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.

If there are any questions, or if additional information is required, please contact Jay Phelps at 361 972-8560.

Sincerely,

FOR

Mike Murray
Manager, Regulatory Affairs

c: The Honorable Allison M. Macfarlane, Chairman, NRC
The Honorable Kristine L. Svinicki, Commissioner, NRC
The Honorable William C. Ostendorff, Commissioner, NRC
The Honorable Stephen Burns, Commissioner, NRC
The Honorable Jeffrey Baran Commissioner, NRC
Mr. Mark A. Satorius, EDO, NRC
Mr. James T. Wiggins, NSIR, NRC
Mr. Barry C. Westreich, NSIR/CSD, NRC