JANET R. SCHLUETER
Senior Director, Radiation and Materials Safety

1201 F Street, NW, Suite 1100
Washington, DC 20004
P: 202.739.8098
jrs@nei.org
nei.org

NUCLEAR ENERGY INSTITUTE

October 26, 2016

Dr. Dennis C. Bley
Chairman, Advisory Committee on Reactor Safeguards
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: ACRS Subcommittee Review of the Proposed Fuel Cycle Facility Cyber Security Rulemaking

Project Number: 689

Dear Dr. Bley:

On behalf of the Nuclear Energy Institute's (NEI)[1] fuel cycle facility (FCF) members, we appreciate the opportunity to submit the following comments for the Advisory Committee on Reactor Safeguards (ACRS) Subcommittee on Digital Instrumentation and Controls consideration for the November 2, 2016 public meeting. I have also contacted ACRS staff to request the opportunity to provide an oral statement that reiterates the industry's concerns described in this letter. NRC staff has held extensive stakeholder interactions and we look forward to continue working towards a rule that is graded, risk-informed, and promulgated in a manner that is consistent with the historical approach and proven framework for the protection of special nuclear material from theft and radiological sabotage.

Industry and NRC share a common objective of ensuring that FCFs are protected from events that may seriously affect the protection of the workers and the public. FCFs have implemented extensive cyber security controls to protect their digital assets for business continuity and regulatory purposes. These controls include meeting the existing NRC security orders requiring that FCFs evaluate and address cyber security vulnerabilities and requirements for Category I facilities to address cyber-attacks through the design basis threat (DBT).

This letter focuses on five areas of concern that we believe need to be resolved prior to the proposed rule being sent to the Commission or be brought to the Commission's attention as policy issues that require

[1] NEI is responsible for establishing unified nuclear industry policy on matters affecting the nuclear energy industry, including regulatory, financial, technical and legislative issues. NEI members include all companies licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect/engineering firms, fuel fabrication facilities, materials licensees, and other organizations and individuals involved in the nuclear energy industry.

direction. At a high level, these issues are regarding: 1) the departure from the historical treatment of special nuclear material security for fuel cycle facilities; 2) a current petition for rulemaking; 3) the excessive burden associated with screening digital assets; 4) the treatment of federally accredited unclassified systems; and 5) alternatives to the rule for licensees that will have no vital digital assets.

Policy Implications of Departing from the NRC's Historical Approach

This rulemaking raises significant policy issues. Specifically, as currently drafted, the rule would impose cyber security requirements on Category II and III licensees not currently subject to the DBTs, and 10 CFR Part 40 FCF licensees that have no requirements under Part 73. The introduction of a cyber-attack as an adversary capability does not justify a substantial departure from the current regulatory framework. This framework is risk informed, outlining graded protection measures based on the NRC's established material categorization and a cyber-attack should not change the attractiveness of this material as a target.[2] The objective of the physical protection programs for Category II and III materials is to minimize the possibility for unauthorized removal of SNM and to facilitate the location and recovery of missing SNM. Facilities with Category II and III materials (and uranium hexafluoride conversion facilities) are not required to protect against the DBTs of theft or diversion and radiological sabotage. The NRC has adopted the reasonable position that un-irradiated HEU, LEU, and natural UF_6 are not considered a sabotage target. This position was most recently reaffirmed in the 2015 Part 73 Regulatory Basis, which states that there is no need for increased physical security protection of these materials. The staff's position in proposed cyber security rulemaking would result in licensees protecting digital assets from a cyber-attack where those same assets are not required to be protected against physical attacks. We believe staff has not adequately demonstrated or justified this major shift in the regulatory framework and this significant departure in policy should be brought to the Commission's attention for direction.

NEI Petition for Rulemaking

In June 2014 NEI submitted a petition, PRM-73-18, that seeks to align the scope of the 10 CFR 73.54 reactor cyber security rule with the underlying agency objective of preventing radiological theft and sabotage. This petition, if granted, has significant policy implications on the direction of the FCF cyber security rulemaking and would essentially scope out Category II, III, and Part 40 licensees. Yet, the staff's final regulatory basis is silent on the PRM. We firmly believe that NRC staff, the ACRS, and the Commission need to be informed of this important policy issue linkage such that a decision on either the PRM or proposed rule are not made in isolation regardless of the timing of either agency decision.

Excessive Burden for Screening Digital Assets

The current draft rule, 10 CFR 73.53(d)(3), requires licensees to identify all digital assets associated with a consequence of concern. To meet the regulation, as outlined in the draft regulatory guide, licensees must first identify potential digital assets associated with a consequence of concern; document this by identifying the asset, describing its function, and describing the applicable consequence of concern;

---

[2] Section 2: Existing Regulatory Framework, Rulemaking for Enhanced Security of Special Nuclear Material, January 2015, Docket NRC-2014-0118

and then apply and document the alternate means criteria to determine if it is a vital digital asset (VDA). Estimates for Category III and Part 40 licensees indicate that up to 1,000 digital assets per facility for screening as potential VDAs; Category I facilities estimate up to 13,000 digital assets will need to be screened. Documenting the screening of 13,000 digital assets is a monumental task, particularly in light of the existing analysis that already identifies the items that are important to safety and security. Licensees have already completed extensive evaluations, such as the Integrated Safety Analysis (ISA) and security plans, that identify the systems that are important to safety and security. This proposed process would require that licensees expand considerable resources to essentially recreate an ISA-like document to identify all digital assets adds a burdensome effort with little to no safety or security benefit. Furthermore, this level of effort is outsized and the NRC staff estimated 12 VDAs per licensee demonstrates the unnecessarily broad starting point for this evaluation.

Recognition of Accredited, Unclassified Systems

Category I fuel facilities currently implement federally-accredited cyber security plans. The draft rule scopes out digital assets that are part of an accredited, classified system, but does not scope out digital assets that are part of a federally-accredited, unclassified system. As a result, Category I licensees estimate that they may need to evaluate up to 13,000 digital assets per facility that fall into the scope of potentially causing a consequence of concern. Licensees are implementing the same NIST controls for accredited classified and unclassified systems. NRC staff is working on the issue and needs to expeditiously resolve it. A resolution would result in a significant decrease in the number of assets to consider as part of this rulemaking while resulting in no measurable decrease in safety or security. In fact, this item may scope all digital assets out of consideration from protection under the proposed rule at some Category I facilities. I believe we share the mutual goal of avoiding dual regulation in this important program area.

Pathway for Licensees with No Vital Digital Assets

Early analysis indicates that Category III, Part 40 licensees, and Category I licensees (pending resolution of accredited, unclassified systems) will have a very small number of VDAs that will fall under the scope of the rule as it is currently proposed. Despite this small number of assets, as the draft rule and guidance are currently written, licensees will be required to develop, implement, and maintain a costly infrastructure to demonstrate initial and continued compliance with the rule. We believe that licensees may decide to implement additional non-digital controls (e.g., administrative controls) simply to avoid having a VDA. NRC staff should create a regulatory pathway for licensees to demonstrate that they have no VDAs, and therefore do not have to proceed with the development of a cyber security plan and cyber security team unless operations change and VDAs are created.

Summary

We appreciate the opportunity to provide industry's perspective on this important rulemaking and trust this information will be useful for the Subcommittee's meeting on November 2, and the full Committee meeting on December 8, 2016. For additional background, please see the two most recent NEI letters on the draft regulatory basis[3] and the NRC staff's preliminary implementation cost estimates[4].

If you have any questions about the content of this letter, please contact me or Nima Ashkeboussi at nxa@nei.org.

Sincerely,

Janet R. Schlueter

Attachment: As Stated

c: Mr. Craig Erlanger, NMSS/FCSE, NRC
Mr. Mark Lesser, RII/DFFI, NRC
Ms. Christina Antonescu, ACRS/TSB, NRC
Mr. Christopher Brown, ACRS, NRC
Mr. James Downs, NMSS/FCSE, NRC
NRC Document Control Desk

[3] Letter from Joseph Pollock (NEI) to Annette Vietti-Cook (NRC) "Fuel Cycle Facility Cyber Security Draft Regulatory Basis", October 5, 2015 (ML15355A449).

[4] Letter from Nima Ashkeboussi (NEI) to Craig Erlanger (NRC) "Comments on Cyber Security Implementation Costs", October 19, 2016.