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

June 9, 2017

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

Subject: ACRS Review of the Proposed Fuel Cycle Facility Cyber Security Rulemaking **NRC Docket: NRC-2015-0179**

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 and attached comments for consideration by the Advisory Committee on Reactor Safeguards (ACRS). Our comments are based on a *preliminary* review of the seven draft NRC documents publicly released to support the June 8, 2017 staff briefing of the ACRS on the subject rulemaking (ML17145A325) and were informed by the staff briefing. Thank you for allowing me to make a statement on behalf of NEI members at the conclusion of today's briefing.

As I stated in my October 26, 2016 letter to you on this rulemaking, industry and NRC share an important common objective of ensuring that fuel cycle facilities (FCFs) are protected from events that may seriously affect the protection of the workers and the public regardless of the initiating event. FCFs have implemented extensive cyber security controls to protect their digital assets for business continuity and regulatory safety and security purposes and, most importantly, these programs continue to evolve. Cyber security 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). We can assure you that industry works tirelessly to ensure the effectiveness of its cyber security programs.

Industry appreciates the eleven NRC public meetings held to date and draft NRC rulemaking documents released in advance of these meetings. Naturally, industry has expressed its views on various aspects of the

[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.

rulemaking during these meetings, by letters and during briefings of the ACRS and its Digital Instrumentation and Control subcommittee. As a result, the staff is fully aware of industry's continuing fundamental concerns with the stated basis for and scope of the current draft rule. We firmly believe that more can and should be done by NRC staff to draft a rule that is more graded and risk-informed, and promulgated in a manner that is consistent with the historical approach and proven regulatory framework for the protection of special nuclear material from theft, diversion and radiological sabotage.

As a result of our preliminary review of the seven documents recently released as background for the June 8, 2017 ACRS briefing by staff, I offer the following regarding industry's current concerns.

Bottom line: *Consistent with NRC's Principles of Good Regulation, NEI and its members firmly believe that the fundamental policy and rule scope issues identified by industry on numerous occasions and described herein should be fully resolved--in consultation with the Commission--prior to submittal of the draft proposed rule for Commission review and approval later this year. Otherwise, the rule scope and its basis could be fundamentally revised during the rulemaking process or, worse case, after implementation of the rule.*

Five Significant Areas of Concern Remain: The five significant areas of concern which were described in my October 2016 letter to you have not been fully resolved to date. While the draft SECY paper recently released mentions these issues in the context of "Stakeholder Interactions", it does not provide a thorough description or discussion of them needed to facilitate a fully informed Commission decision on these matters.

At a high level, the five issues are regarding: 1) the staff's departure from the historical treatment of special nuclear material security for fuel cycle facilities; 2) an unresolved and related petition for rulemaking (PRM-73-18); 3) the unnecessarily 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. In some respects, the most troubling item is issue 2 above. Specifically, the staff acknowledges on page 8 of the draft SECY that if NRC decides to grant PRM-73-18, the staff would <u>then</u> determine whether and how the scope of the FCF cyber security rule would be narrowed and thus future rule revisions might be necessary. Such an approach is unnecessarily resource intensive, confusing, disruptive, not predictable or consistent with NRC's principles of good regulation and, in our opinion, ill-advised. Rather, the staff should make those critical rule scope determinations <u>now</u> to facilitate fully informed staff and Commission decisions on the proposed rule under development. *A full discussion of all five areas of concern is attached and was included in the NEI letter to you dated October 26, 2016.*

Sample of Preliminary Comments on Draft Documents Recently Released: While we recognize that the documents were not released for official public comment, we nevertheless reviewed them to better understand their development and, as such, we offer a few key insights for your consideration. A sample of our preliminary observations are as follows: 1) Use of the post-9/11 security orders as a basis for applying the rule to all FCFs is weak, in that, unlike the rulemaking process under the Administrative Procedures Act, a regulatory safety basis is not procedurally required to issue security related Orders. In addition, the Commission disapproved a staff recommendation in 2014 to issue Orders to FCFs in lieu of rulemaking in the absence of a common defense and security basis (SRM on SECY-14-0147). It should also be recognized

that the earlier Orders required licensees to identify critical target areas (CTAs) and only the Category I facilities identified CTAs. In disapproving the 2014 Orders, the Commission directed that staff engage stakeholders and pursue a graded, consequence-based approach to the rulemaking. We would argue that this goal has not yet been met; 2) on a related note, the SECY does not but should describe when and how the existing NRC security Orders would be rescinded; 3) while the staff doubled their rule implementation cost estimate to over $545K per licensee, it is still well below the earlier industry estimate of $1.8M per licensee to implement plus ongoing maintenance costs for compliance and, one could argue based on the current draft guidance that our earlier estimate is low; 4) licensees have an established configuration management program in place (i.e., 10 CFR 70.72); therefore, it is unclear why a separate configuration management requirement is proposed; 5) the basis for the estimate of 12 VDAs average per FCF has not been provided to date and, as we have stated, is very likely an underestimate by 100 fold (if federally accredited unclassified systems are not scoped out) for some licensees; 6) the draft regulatory guide essentially requires that licensees expend considerable resources to create an Integrated Safety Analysis-like document to identify items important to safety and security for the purposes of cyber security. It is unclear why this is necessary since the ISA has already identified items relied on for safety; 7) the cyber security template in Appendix A to the draft regulatory guide goes way beyond the proposed rule requirements, e.g., suggesting licensees test incident response capabilities and propose a testing frequency; 8) it is not clear how or why NRC expects licensees to account for the potential cumulative effects that could result from the simultaneous compromise of several digital assets from a cyber attack; 9) the draft regulatory guide refers to “attack vectors” but does not enumerate them; 10) the definition of a cyber attack needs revision in that it states that a cyber attack is a physical attack. The basis for this definition is not clear; 11) the security controls catalog should be eliminated and, if necessary, be replaced with a table that simply marks which controls are applicable to which consequence of concern; and 12) it is unclear how licensees would address cyber security controls that address attack vectors against which a licensee is not required to defend. These twelve examples are a sample of our preliminary observations to date, but represent significant scope and implementation concerns including the resources needed to address them.

Backfit Analysis: We appreciate the somewhat unprecedented level of detail and discussion contained in the draft backfit analysis recently released. Based on a preliminary review, we are concerned with certain aspects of it, including the adequate protection analysis and methods used to quantify the benefits associated with the propose rule. Therefore, while this is a very important aspect of the rulemaking, and we look forward to the NRC’s Committee to Review Generic Requirements’ review, we offer no further comment on this analysis at this time and will continue to review it.

Summary

We appreciate the opportunity to provide industry’s perspective on this important rulemaking and trust this information will be useful for the ACRS deliberations. As stated, we have fundamental concerns regarding the scope of this rule and its implementation and will continue to engage the NRC staff, senior management and Commission on these matters. For additional background beyond my October 2016 letter to you, please

see the NEI letters on the draft regulatory basis[2] and the NRC staff's preliminary implementation cost estimates[3].

If you have any questions about the content of this letter, please contact me or William Gross, director of Emergency Preparedness and Incident Response at 202.739.8123 or wrg@nei.org.

Sincerely,

Janet R. Schlueter

Attachment

c: Mr. Frederick Brown
Mr. Marc Dapas
Mr. Craig Erlanger
Mr. Mark Lesser
Ms. Christina Antonescu
Mr. Christopher Brown
Mr. James Downs
Mr. Norman St-Amour
NRC Document Control Desk

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

[3] Letter from Nima Ashkeboussi (NEI) to Craig Erlanger (NRC) "Comments on Cyber Security Implementation Costs", October 19, 2016 (ML16315A290).

Five Significant Policy and Scope Areas of Concern with Current Draft Proposed Rule for Cyber Security at Fuel Cycle Facilities – June 2017

[From the October 26, 2016 NEI letter to ACRS]

1. 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.[1] 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.

2. 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.

3. 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

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

describing the applicable consequence of concern; 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.

4. 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.

5. 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.