

**JOSEPH E. POLLOCK**  
*Vice President, Nuclear Operations*

1201 F Street, NW, Suite 1100  
Washington, DC 20004  
P: 202.739.8114  
jep@nei.org  
nei.org



October 5, 2015

Annette Vietti-Cook  
Secretary  
U.S. Nuclear Regulatory Commission  
Washington, DC 20555-0001

**Subject:** Fuel Cycle Facility Cyber Security Draft Regulatory Basis (80 Fed. Reg. 53478); Docket ID NRC-2015-0179

**Project Number: 689**

On behalf of the Nuclear Energy Institute's (NEI)<sup>1</sup> fuel cycle facility members, we submit the following comments on the Nuclear Regulatory Commission's (NRC) draft Regulatory Basis for a potential rulemaking that would adopt new cyber security requirements for fuel cycle facilities. On September 4, 2015, NRC published a notice in the Federal Register requesting public comment on the draft Regulatory Basis by October 5, 2015. On September 23, 2015, NRC held a public meeting to discuss the draft Regulatory Basis. The public discussions were informative and provided industry the opportunity to discuss most of the comments contained in this letter.

**The Draft Regulatory Basis Does Not Justify Rulemaking**

Cyber security is a matter of great national importance. Industry and NRC share a common objective of ensuring that fuel cycle facilities are protected from events that may seriously impact workers, the public, and the environment. As such, we firmly believe that NRC should treat a potential cyber attack like it would treat any other potential initiating event that could also trigger an accident sequence. Licensees have significant expertise in evaluating and mitigating the consequences of accidents through processes, procedures, systems, structures, and components. Significant work and analysis is needed to continue with this effort as the draft Regulatory Basis does not provide a sufficient technical basis to justify rulemaking. In addition to protecting their digital assets for business purposes, licensees are subject to existing security orders requiring that they evaluate and address cyber security vulnerabilities. Further, Category I licensees must protect digital assets for the Design Basis Threat (DBT), which specifically includes a cyber attack. Industry has spent, and continues to spend, significant resources on implementing cyber security programs. These programs continue to evolve in response to changing environments and have sufficiently mitigated the consequences of cyber security breaches without added rulemaking. We trust that this fact is self-

---

<sup>1</sup> The Nuclear Energy Institute (NEI) is the organization responsible for establishing unified industry policy on matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include all entities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect/engineering firms, fuel cycle facilities, nuclear materials licensees, and other organizations and entities involved in the nuclear energy industry.

evident to NRC as it conducts the site visits currently underway. Rather than dismiss these programs as ad hoc, NRC should evaluate the extent to which existing requirements, in conjunction with ongoing voluntary practices, address the regulatory problem set forth in the draft Regulatory Basis.

### **Policy Implications of Departing from the NRC's Historical Approach**

The cyber threat for fuel cycle facilities should be informed by and consistent with NRC's established approach and proven framework for the protection of special nuclear material (SNM). The introduction of a cyber attack as an adversary capability should not require a substantial departure from the current regulatory framework for grading protection measures based on the NRC's established material categorization approach based on risk informed regulation.<sup>2</sup>

First, the draft Regulatory Basis appears to depart from NRC's historical approach of reflecting the different risks associated with different categories of fuel cycle facilities through different regulatory requirements. The rationale underlying the NRC's security regulations is that protective measures should be commensurate with the potential consequences of malevolent acts to safety and security. The basis for issuing requirements to defend against cyber attacks at fuel cycle facilities that are not currently subject to the DBT requirements in 10 CFR 73.1 must be carefully considered to avoid the unintended adverse effects on diverting limited resources to a single stand-alone focus on cyber security. Rather than follow this traditional approach, the draft Regulatory Basis takes a one-size-fits-all approach of applying cyber security regulations to all fuel cycle facilities regardless of their risk profile, and instead NRC would seek to grade the requirements through implementation guidance. The draft Regulatory Basis does not address this policy issue. While a graded implementation is reasonable, prudent, and desirable, as a matter of policy, NRC should establish requirements reflecting the diverse range of fuel cycle facilities at outset through the rulemaking process rather than deferring this issue to guidance.

Second, the draft Regulatory Basis proposes creating requirements that have no nexus to the recognized risks for Category II and III facilities. 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<sub>6</sub> 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. But here, the draft Regulatory Basis and 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. This inconsistency in regulatory approach should not be dismissed without further evaluation. Further, it implies that the threat and consequences of a cyber attack are greater than a physical attack. The draft Regulatory Basis provides no evidence justifying this major shift in the regulatory framework. Before proceeding with a rulemaking, we believe NRC must justify this significant change in its approach to security and address this policy issue.

Third, Category II and Category III licensees are under orders to identify "Critical Target Areas" (CTAs). A CTA is described as an area that if subjected to a malevolent act, could potentially result in a lethal exposure from radiological material or chemicals subject to NRC regulation to members of the public located

---

<sup>2</sup> Section 2: Existing Regulatory Framework, Rulemaking for Enhanced Security of Special Nuclear Material, January 2015, Docket NRC-2014-0118

outside of the Owner Controlled Area.<sup>3</sup> Licensees used guidance provided by the NRC to identify CTAs and to implement specified protection criteria, if necessary. The NRC has reviewed licensee assessments and implementation of protection measures. No Category III fuel cycle facility has identified a CTA. Industry is not aware of any NRC generic or site-specific vulnerability assessments indicating any cyber threat actuating significant impact on actual safety or security of the public that would justify the current cyber security rulemaking effort. The development of CTAs in accordance with the post-9/11 orders could constitute a reasonable surrogate for a site-specific vulnerability assessment. In the absence of a cyber-specific vulnerability assessment, it seems unreasonable to conclude a cyber attack on a Category III fuel cycle facility could create a CTA that does not otherwise exist. Accordingly, it would appear that requirements to protect against acts of cyber sabotage are simply not justified by the risks.

The NRC's regulations under Part 73 do not apply to Part 40 licensees. Nonetheless, Part 40 licensees are required by order to identify CTAs and have not identified any CTAs.

### **Recent Commission Direction**

In SRM-SECY-14-0147, the Commission disapproved the staff's recommendation for cyber security orders and directed the staff to initiate a cyber security rulemaking to develop a more fulsome technical basis. Commissioner Ostendorff's vote noted that the "staff has not provided a sufficient basis for the Commission to make a finding that the fuel cycle facilities regulatory functions are not currently protected in a manner sufficient to adequately protect public health and safety." The current draft Regulatory Basis falls far short of providing a detailed rationale to demonstrate that fuel cycle facilities are not adequately protected today. For example, rather than provide significantly new information or a more fulsome assessment of the issues, the draft Regulatory Basis is based on information gathered from site visits in 2011 and discusses cyber event consequences in a vague, non-specific manner. Also, the draft Regulatory Basis continues with an isolated focus on a stand-alone cyber attack. We believe that this approach is not responsive to the SRM direction of ensuring an adequate, integrated look at cyber security as only one aspect of site security. Most importantly, is the draft Regulatory Basis definition of a cyber attack as "having the potential to result in a direct or indirect adverse effect or consequence to a digital asset or system." The purpose of rulemaking and cyber security should be more properly directed to protect against a cyber attack that results in a safety or security consequence of a concern, and not simply a consequence to a digital asset. This broad scope mindset of including all digital assets is not consistent with a risk informed, graded approach focused on consequences as directed by the SRM. The need to tightly align consequences with the scope of assets protected is at the heart of what has been identified as the most significant lesson learned from implementation of the cyber security requirements for power reactors, and resulted in NEI submitting a petition for rulemaking (PRM-73-18). We have emphasized to NRC on several occasions that such lessons learned must be applied to avoid undue burden to both NRC and industry in this regulatory initiative.

### **Cost Implications and Backfit Concerns**

The draft Regulatory Basis provides no substantive discussion of the backfitting considerations, and dispenses with any meaningful costs justification to an unsubstantiated conclusion that, "a rulemaking to implement cyber security requirements for FCF licensees will have a number of benefits that justify the potential cost impacts both on the licensee and the NRC." This improper justification implies that whatever the cost to licensees, the safety and compliance benefits of the rulemaking are worth it. At best, this

---

<sup>3</sup> Attachment 1, Page 26 of 30; Luminant Response to Request for Additional Information, February 17, 2014 (ML14051A437)

rulemaking would marginally improve safety but at great financial cost and at the expense of other licensee self-identified operational improvements, which on a site-specific basis often have a higher rate of return to safety. At a closed Commission briefing in February 2014, two power reactor licensees provided a detailed description of their current expenditures required to comply with the power reactor cyber security requirements. Both licensees indicated that the current and projected full program implementation costs *substantially exceed* the cost estimates provided in the regulatory analysis for the rulemaking included in Enclosure 2 to SECY-08-0099 (July 9, 2008). The regulatory analysis for reactors estimated a one-time cost for program establishment of \$1,194,200 per site. A key driver for the costliness of compliance is the large number of digital assets identified for protection against cyber attack that have no nexus to preventing radiological sabotage. Given the draft Regulatory Basis could require fuel cycle facilities to protect an even broader set of assets than the power reactors, it is reasonable to conclude that the costs to fuel cycle facility licensees will be considerable. The cost implications for Category II and Category III licensees may be even greater given these facilities do not have NRC-required access authorization, physical protection, and insider mitigation programs that the reactor and Category I licensees may credit for affording a certain degree of cyber security protection. Unless cyber security requirements are justified by a *substantial increase* in *overall* protection of public health, safety, or security, and the implementation costs for facilities are justified in view of this increased protection, NRC should not proceed with this rulemaking.

### **Specific Rulemaking Recommendations**

If rulemaking continues, industry makes the following recommendations:

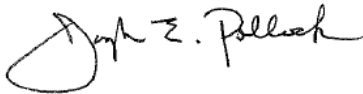
- 1) Specifically address the significant policy issues discussed above, given the lack of analysis that demonstrates the risk for Category II, Category III, and Part 40 fuel cycle facilities. Demonstrate that the shift in the regulatory framework from physical security requirements to cyber security requirements is justified based on increased consequences to the public, worker, or environment.
- 2) Provide clear performance objectives, similar to those found in 10 CFR 70.61, in the Regulatory Basis and rule. Industry provided a comprehensive proposal for a path forward in October 2013. This proposal provided a regulatory basis citing consistency with existing rules, guidance and policy. It contained explicit objectives complimented with clear criteria that enhance the implementation process as well as the inspection of the assessments warranted. The proposal also provided a screening logic that provided a road map for risk informing the assessment to assure the protection of the public, worker and environment. NRC did not provide feedback or a justification on why this proposal was not adequate. We suggest adoption of this approach as opposed to the current path.
- 3) As discussed above, the rulemaking should be "right sized" from the beginning with the end state in mind. Currently, the draft Regulatory Basis casts a wide net capturing all digital assets and relies on screening contained in guidance to ensure the "right end state" of targeted digital assets will reveal itself. The scope of assets identified in the regulations requiring protection should only extend to those most necessary to prevent theft or sabotage of SNM. NEI recommends that NRC consider the specific recommendations in PRM-73-18 (79 FR 183, dated September 22, 2014) as a basis for the scoping provisions. We believe this recommendation is consistent with SECY-14-0147, which states: "The results of this [PRM] activity will be considered to the extent relevant to FCFs if rulemaking is pursued for FCFs." The Regulatory Basis should address the need to integrate the regulatory consideration of safety and security and the necessity to apply a disciplined, graded approach to the identification of digital assets and a graded, consequence-based approach to their protection.
- 4) Rather than issuing specific cyber reporting requirements, the NRC should carefully assess existing reporting requirements applicable to fuel cycle facilities to determine if they are adequate to cover reporting of cyber security events since such requirements focus on the safety/security results of a

failed safety device regardless of the initiating event. Existing guidance on applicable reporting requirements could be revised to address cyber events.

- 5) In the Regulatory Basis, NRC should provide a quantitative assessment on the consequences of a cyber security event. In its absence, industry is considering whether it should convene an expert panel to quantify the risks from a cyber attack. Based on our consideration of this issue to date, preliminary indicators could lead to a conceivable finding that a minimal, if any, increased safety margin is gained following implementation of the approach described in the draft Regulatory Basis.
- 6) Any new regulation should not apply to all digital assets managed by a licensee under the purview of another agency's oversight (e.g. DOE, NNSA, DOD) that are accredited under an established national consensus standard or that other agency's cyber program. Otherwise these program areas will be subject to unnecessary dual regulation. Therefore, the final rule and regulatory basis should include a specific exemption for these licensee programs.
- 7) Part 73 requires that certain licensees protect SNM. However, these requirements do not apply to Part 40 licensees. Accordingly, uranium hexafluoride conversion facilities should be explicitly excluded from this rulemaking. The lack of an identified CTA is indicative of the low risk to the safety and security of these facilities from a cyber attack clearly supports this exclusion.

Attached are specific industry comments based on our review of the draft Regulatory Basis and the questions posed to stakeholders in the FRN. We appreciate your consideration of these comments. If you have any questions, please contact me, Nima Ashkeboussi (202.739.8022; [nxa@nei.org](mailto:nxa@nei.org)) or Bill Gross (202.739.8123; [wrg@nei.org](mailto:wrg@nei.org)).

Sincerely,



Joseph E. Pollock

Attachments: As stated

- c:
- Ms. Catherine Haney, NMSS, NRC
  - Ms. Marissa Bailey, NMSS/FCSE, NRC
  - Mr. Brian Smith, NMSS/FCSE, NRC
  - Mr. Brian Holian, NSIR, NRC
  - Mr. James Anderson, NSIR/CSD, NRC
  - Ms. Carrie Safford, OGC/GCLR/HLWFCNS, NRC
  - Mr. Norman St. Amour, OGC/GCLR/HLWFCNS, NRC