NIMA ASHKEBOUSSI
Senior Project Manager, Radiation and Materials Safety

1201 F Street, NW, Suite 1100
Washington, DC 20004
P: 202.739.8022
nxa@nei.org
nei.org

NUCLEAR ENERGY INSTITUTE

October 19, 2016

Mr. Craig Erlanger
Director, Division of Fuel Cycle Safety, Safeguards & Environmental Review
Office of Nuclear Material Safety and Safeguards
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Fuel Cycle Facility Cyber Security Implementation Costs

Project Number: 689

Dear Mr. Erlanger:

On behalf of the Nuclear Energy Institute's (NEI)[1] fuel cycle facility (FCF) members, we submit the following comments and inputs on the U.S. Nuclear Regulatory Commission (NRC) staff's draft implementation cost estimates for the fuel cycle cyber security proposed rulemaking package. We appreciate NRC management's support of the staff's extensive stakeholder interactions, including the public meeting on October 12, 2016 to discuss this rulemaking and these estimates. While industry remains concerned about certain rule elements, we firmly believe the meetings have led to a better understanding of the draft proposed rule and closer alignment on some mutual issues of concern. As such, we encourage continued, extensive outreach on this important rulemaking.

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. It is important that this rulemaking reflect the NRC's well-established practice of addressing cyber security in a risk-informed manner for FCFs and the measures that are in place to address cyber security concerns at these facilities. In fact, FCFs have implemented extensive cyber security controls to protect their digital assets for business continuity and regulatory purposes, in addition to existing NRC security orders requiring that FCFs evaluate and address cyber security vulnerabilities and the design basis threat (DBT) cyber threat addressed at Category I facilities.

[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.

Policy Issue

It is important to note that this rulemaking raises significant policy issues. Specifically, as currently drafted, the rule would impose cyber security requirements on licensees not currently subject to the DBTs, including 10 CFR Part 40 licensees that have no requirements under Part 73. Additionally, there is an NEI petition for rulemaking, PRM-73-18, that seeks to align the scope of the 10 CFR 73.54 cyber security rule with the underlying agency objective of preventing radiological sabotage. Resolution of these two issues has significant implications for the ultimate direction and scope of any FCF-specific cyber security rulemaking and associated implementation. Therefore, we firmly believe that this rule should not move forward in isolation but, rather, the proposed and final FCF-specific cyber security rule should reflect the NRC's final decision on the PRM and the inherently important policy issue discussed above.

Industry Cost Estimate

While we recognize that the material provided is a draft and work in progress, we have concerns that the current NRC estimated implementation costs of $273,000 per licensee significantly underestimates these costs. Among other things, this concern is based on the program expectations outlined in the draft regulatory guide, FCF experience with implementing cyber security controls under other federal agency programs, and the experience of 10 CFR Part 50 licensees with cyber security requirements under 10 CFR 73.54. In fact, we estimate that this rule will cost the fuel cycle industry $14.2 million to implement in addition to annual costs to maintain compliance. Industry's implementation cost estimates are conservative, based on our interpretation of the material presented during NRC's public meeting on August 25, 2016, and does not reflect the content of any discussions during the meeting which may lead to future changes in the draft rule or regulatory guide. Therefore, similar to the staff's preliminary cost estimates, our planning assumptions may change as the rule language and regulatory guide evolve. The costs range from $892,000 to $2.8 million per facility, with an average implementation cost of $1.8 million. As we noted during the October 12, 2016 public meeting, there are at least two key points on this estimated cost range. First, the category of licensee is not indicative of its cost range and secondly, there is not a direct correlation between the number of vital digital assets (VDAs) and program costs since there can be some economy of scale at some sites. Also, NRC initial estimates do not account for the costs beyond the first year of implementation even though additional costs will be necessary to maintain a new regulatory program as outlined in the draft proposed rule and regulatory guide. Some maintenance costs are estimated in the attachment.

Cyber Security Plan

The NRC cost analysis for creating the cyber security plan assumes that there will be no costs associated with the creation of the cyber security team (CST). While some licensees may have individuals onsite that meet the regulatory guide's expectations for CST qualification and staffing levels, a large number of licensees will need to hire staff or contractors to fill these roles or hire additional staff to fill the roles of current staff that will now have CST duties to meet the prescriptive nature of the draft proposed rule. This process requires time and resources, with the industry average cost of $20,000 to hire one new staff member or contractor.

NRC's Table 4-1 estimates the labor hours to develop the cyber security plan with the effort estimated at 400 total hours per facility. Our average estimate for completing this task is 690 total hours per facility. The attachment outlines the revised hourly estimates per role for this task. This estimate is largely informed by the knowledge from Category I licensees who have experience with developing cyber security plans and their associated policies and procedures for accreditation by other federal agencies. Furthermore, all FCF have general experience with the level of effort related to the development of regulatory plans under NRC authority.

Finally, the labor rates used to calculate the estimate in this table and throughout the document do not reflect the true costs that licensees compensate for these positions in today's market. The hourly industry average rate for the five positions listed in the table is in the attachment. The industry estimates the cost of creating the cyber security plan to be $76,350 per facility.

Analysis of 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; and then apply and document the alternate means criteria to determine if it is a VDA. This is a substantial effort and the associated costs are significantly underestimated in Table 4-2.

Category I fuel facilities currently implement federally-accredited cyber security plans. As part of the rule, these licensees must consider all DBT and safety digital assets. 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. A preliminary estimate indicates there may be up to 800 VDAs per facility. Documenting the screening of 13,000 digital assets is a monumental task. In SECY-16-0105, NRC staff reaffirmed "that dual regulation can reduce regulatory certainty and has taken steps to avoid or minimize dual regulation. In cases where another government agency is issuing rules that impact NRC licensees, the NRC has provided its perspectives on the need to avoid dual regulation throughout the rulemaking process."[2] NRC needs to expeditiously resolve this issue. A resolution could 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. If unchanged, Category I licensees will have significantly more VDAs than the NRC currently estimates; thus NRC will need to justify this increased regulatory burden and associated costs.

Per the draft rule, Category III and Part 40 licensees must consider digital assets associated with safety systems and classified information. However, all licensees (including Category I) have already completed extensive evaluations through an Integrated Safety Analysis (ISA) to identify the systems that are important

[2] SECY-16-0105, " Staff Assessment of Issues Raised in Commission Meeting With Stakeholders", September 15, 2016, Page 6.

to safety (i.e. items relied on for safety and plant features and procedures) and linked to the consequences of concern as defined in 10 CFR Part 70. In light of the existing analysis that already identifies the items that are important to safety and security, the proposed two step process to identify all digital assets and then apply the screening criteria adds a burdensome effort with little to no safety or security benefit. The process outlined in the regulatory guide would require that licensees expand considerable resources to essentially recreate an ISA-like document. A preliminary estimate for Category III and Part 40 licensees indicates that step one of this process may require that these licensees identify up to 1,000 digital assets per facility for screening as potential VDAs. The NRC's cost implementation document estimates that once FCFs screen these digital assets during the second step of this process, licensees will have identified only 12 VDAs. While the basis for this low number is not clear, we expect that Category III and Part 40 licensees will have very few VDAs. This demonstrates the unnecessarily broad starting point for this evaluation, particularly given the existing information already available in licensee ISAs.

Based on the current draft rule and regulatory guide, an estimated level of resources needed to identify, document, and screen all digital assets associated with a consequence of concern is $244,000 per facility. This estimate is based on the number of digital assets that must be analyzed to identify VDAs the level of effort to create another ISA-like cyber security document for the sole purpose of this rule. Detailed hourly estimates are in the attachment.

Vital Digital Assets

After applying the screening methodology, licensees will have to document, apply controls as necessary, and address how each VDA meets the control objectives outlined in the draft regulatory guide. The control sets are informed by the NIST controls for information systems and guide to industrial control system security (NIST SP 800-53 and 800-82). Currently, the number of controls to be considered for VDAs in the regulatory guide is excessive compared with the desired state to prevent a consequence of concern. This adds a burdensome review and documentation process with no added safety or security benefit. Industry estimates that the cost for addressing controls for VDAs identified in the regulatory guide is $302,000 per facility.

Summary

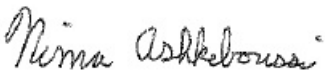
We appreciate the advanced opportunity to provide input into the implementation cost estimates prior to the draft rule going to the Commission for review and trust this information will be used to inform the document. The cost/benefit justification to support the current regulatory approach is not apparent at this time. Based on the data provided in this letter and attachment, this rule will cost the industry $14.2 million to implement plus additional annual costs to maintain compliance that the NRC estimate does not account for, including the costs of NRC inspection. Further, industry is concerned that inspection costs might be further escalated due to the use of contractors who are not familiar with the sites. Early analysis indicates that Category III and Part 40 licensees will have a very small number of VDAs that will fall under the scope of the rule as it is currently proposed. If accredited, unclassified systems are scoped out of the rulemaking, Category I licensees will also have a very small number of VDAs. Despite this small number of assets,

licensees will be required to develop, implement, and maintain a costly infrastructure to demonstrate initial and continued compliance with the rule.

Ultimately, licensees may decide to implement new or additional non-digital controls simply to avoid having a VDA, e.g., administrative controls. NRC implementation cost estimates should account for this non-safety or security related expense caused by licensee actions to implement non-digital controls in response to the rule. These costs could be minimized, however, if the NRC created a regulatory pathway for licensees to demonstrate that they have no VDAs, and therefore did not have to proceed with the development of a cyber security plan and cyber security team unless operations change and VDAs are created.

We look forward to working with you and your staff as this rulemaking progresses and continue to strongly encourage extensive public outreach. If you have any questions about the content of this letter, please contact me to avoid any misunderstandings that might manifest themselves in the proposed rule or supporting documents.

Sincerely,



Nima Ashkeboussi

Attachment: As Stated

c: Mr. Marc Dapas, NMSS, NRC
Mr. James Andersen, NSIR/CSD, NRC
Mr. James Downs, NMSS/FCSE, NRC
Mr. Matthew Bartlett, NMSS/FCSE/ECB, NRC
Ms. Cardelia Maupin, NMSS/MSTR/RPMB, NRC
Mr. Norman St. Amour, OGC/GCLR/HLWFCNS, NRC
NRC Document Control Desk

A-1. Industry Implementation:

Cyber Security Plan (10 CFR 73.XXX)

The licensee will need to establish a CST responsible for the execution of the cyber security program. The CST will establish, and implement the cyber security plan. It is assumed that the licensee will not incur any cost in creating the CST.

Comment [NXA1]: This is an incorrect assumption. See comment letter and estimate in Table 4-1.

In developing the cyber security plan, the CST will identify and analyze site-specific conditions that impact the implementation of the cyber security program. For the purpose of this analysis it is assumed the licensees will utilize the NRC cyber security plan template and cyber security controls.

The licensee will incur the cost to create the cyber security plan as well as the cost of implementation. This includes the cost to conduct the analysis to identify digital assets, apply the alternate means of control, determine the vital digital assets, and apply cyber security controls to unique vital digital assets. In addition, the licensee will implement compensatory measures to address controls which cannot be implemented as originally intended.

Table 4-1 Creation of the Cyber Security Plan

Create the Cyber Security Plan	Labor hours	Mean/Best cost estimate
creation of the team	0	$40,000~~$0~~
Hours to develop cyber security plan (Security Mgr.)	70~~40~~	$8,750(~~$4,00~~
Hours to develop cyber security plan (cyber security expert)	~~120~~220	$27,500(~~$8,0~~
Hours to develop cyber security plan (Facility expert)	140~~60~~	$17,500(~~$2,5~~
Hours to develop cyber security plan (Safety operations expert)	140~~60~~	$15,400(~~$3,6~~
Hours to develop cyber security plan (licensing/ADM)	120	$7,200(~~$4,53~~
Per FCF		$76,350(~~$22,8~~
Number of licensees		8
Total		$610,800(~~$182,906~~)

Comment [NXA2]: Estimating 2 new employees at $20,000 per person

Comment [NXA3]: $125/hr

Comment [NXA4]: $125/hr

Comment [NXA5]: $110/hr

Comment [NXA6]: $110/hr

Comment [NXA7]: $60/hr

Analysis of digital assets

The licensees will need to conduct an analysis to identify digital assets, consider alternate means of control and determine the vital digital assets. Licensees analyze digital assets used throughout the facility to determine their potential to be compromised by a cyber attack resulting in a consequence of concern. The analysis would distinguish between digital assets that can be protected by alternate means (e.g., a physical barrier), and vital digital assets which require application of the cyber security controls, identified in the cyber security plan, to prevent the consequence of concern.

Table 4-2 Analysis of digital assets

Analysis to identify digital assets, consider alternate means of control, determine the vital digital assets,	Labor hours	Mean/Best estimate
Labor hours (Security Mgr.)	20080	$25,000($8,123)
Labor hours (cyber security expert)	900400	$112,500($26,898)
Labor hours (Facility expert)	650200	$71,500($8,607)
Labor hours (Safety operations expert)	250200	$27,500($12,054)
Labor hours (licensing/ADM)	12080	$7,200($3,023)
Per FCF		$243,700($58,705)
Number of licensees		8
Total		($469,637$1,949,600)

Comment [NXA8]: Using same hourly rates at Table 4-1

Address cyber security controls and written procedures for application of cyber controls to vital digital assets

In addition, the licensee will need to apply and document the alternate means for applicable digital assets and the cyber security controls for vital digital assets. This includes establishment of written procedures for the application of cyber security controls for each vital digital asset. Development of the procedures also need to address the methods to identify cyber attacks on the vital digital asset and incident response, if required. The number of digital assets protected by alternate means will vary by licensee. The FCF are estimated to have an average of 12 vital digital assets per facility.

Comment [NXA9]: The costs of applying alternate means to avoid having a VDA should be considered as part of the implementation costs. If a licensee is taking action as a result of the rule, that cost should be considered; even though it is a cost to avoid the rule.

Table 4-3

Address cyber security controls and written procedures for application of cyber controls to vital digital assets	Labor hours	Mean/Best es
Labor hours (Security Mgr.)	24080	($8,123)$30
Labor hours (cyber security expert)	4001000	($26,898)$125,000
Labor hours (Facility expert)	200750	($8,607)$82,500
Labor hours (Safety operations expert)	200500	($12,054)$55,000
Labor hours (licensing/ADM)	120160	($4,534)$9,600
Per FCF		($60,216)$302,100
Number of licensees		8
Total		($481,728)$2,416,800

Comment [NXA10]: Same labor rate as previous tables.

Other Cyber Security implementation cost

The FCFs will need to train their personnel and make hardware modifications as a result of the proposed action.

Training

It is assumed the cyber security implementation training will entail the creation of the training materials as well as the labor cost to train all necessary personnel. The licensee will incur cost to create and delivering the training of an estimated $$6,000~~2,000~~. It is assumed the training will average 1 labor hours per licensee personnel. The number of personnel will vary by licensee, however it is estimated that the average total cost of training per FCF is estimated to ~~$9,000~~$13,500. For an overall per FCF training cost of non-CST members of $~~11,000~~19,500.

Hardware and installation modifications

It is estimated to cost each FCF on average $120,000 to make the hardware and installations modifications necessary to be in compliance with the proposed regulations. This is based on an estimate of $5,000 to $15,000 for hardware and modifications upgrades for each of the previously assumed 12 vital digital assets (e.g., monitoring and associated anti-malware software).

Table 4-4 Other Industry Implementation Cost

Other Cyber Security Implementation cost	Mean/Best estimate per FCF	Total Cost
CST Training	$40,000~~($11,000)~~	~~($88,000)~~$320,000
Non-CST Training	$19,500	$156,000
Biennial Review	$30,000	$240,000
Hardware and installation modifications	~~($120,000)~~$600,000	~~($960,000)~~$4,800,000
System Testing	$100,000	$800,000
Software	$300,000	$2,400,000
NRC fee recovery for review and approval of cyber security plan	$52,600	$420,000
Records Management	$10,000	$80,000
Number of licensees		8
Total	~~($131,000)~~$1,152,000	~~($1,048,000)~~ $8,416,000

Comment [NXA11]: NRC should add costs for inspection. Conservatively this cost will be 4 inspectors, 80hrs (prep/inspection/documentation), $263/hr is $85,000.

Comment [NXA12]: We estimate that CST staff will require an average of $8,000/member in training prior to implementation. At a minimum, there will need to be at least 5 cyber security support staff to segment responsibilities appropriately per the Reg. Guide. Note: Average SANS course cost $5,500 per class plus other expenses for travel

Our average estimate is that it will take 40 hrs to create the training @ $150/hr. Initial CST training will be one day.

Comment [NXA13]: Conservatively estimating 1hr training for 300 employees, @ $45/hr

Comment [NXA14]: There is a significant difference between the estimated VDAs at Category 1 facilities vs other FCF. We are conservatively estimating $50,000 for hardware modifications.

Comment [NXA15]: $8000; 5 members

Comment [NXA16]: $9000 + $6000 development

Comment [NXA17]: If licensees chose to add additional, non-digital controls to avoid having a VDA, their costs may be close to the costs of applying the hardware/software controls.

Comment [NXA18]: The Reg Guide outlines a very prescriptive testing frequency. Industry estimates a significant number of hours to complete this testing, while we believe in some instances may introduce vulnerabilities in the system. We estimate 1000 labor hours related to testing @ $100/hr on average.

Comment [NXA19]: VA, SIEM, Intel, Host-based

Comment [NXA20]: Based on previous experience with NRC review & approval invoicing, we anticipate 200 billable hours @ $263/hr

Table 4-5 Total Industry Implementation Cost

Total Licensee Implementation Cost	Mean/Best estimate per FCF	Total Cost
Cyber Security Plan	~~($23,000)~~$76,000	~~($183,000)~~$608,000
Supporting technical information	~~($59,000)~~$244,000	~~($470,000)~~$1,952,000
Procedures for cyber security for vital digital assets	~~($60,000)~~$302,000	~~($482,000)~~$2,416,000
Training and hardware modification, and other implementation costs	~~($131,000)~~$1,152,000	~~($1,048,000)~~$9,217,000
Total	~~($273,000)~~$1,774,000	~~($2,183,000)~~$14,192,000

*Note dollars are rounded to the nearest 1,000th