August 31, 2017

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

SUBJECT: DRAFT PROPOSED RULEMAKING FOR TITLE 10 OF THE *CODE OF FEDERAL REGULATIONS* 73.53, "REQUIREMENTS FOR CYBER SECURITY AT NUCLEAR FUEL CYCLE FACILITIES," RELATED PARTS 70, 73, AND 40, AND DRAFT REGULATORY GUIDE DG-5062, "CYBER SECURITY PROGRAMS FOR NUCLEAR FUEL CYCLE FACILITIES"

Dear Dr. Bley:

I am writing in response to a letter, dated June 21, 2017, from the Advisory Committee on Reactor Safeguards (the Committee) (Agencywide Documents Access and Management System Accession Number ML17171A209). The letter addressed the Committee review of the proposed rule package and draft regulatory guide regarding cyber security at fuel cycle facilities.

COMMITTEE'S RECOMMENDATIONS

The staff's responses are below:

Committee Recommendation 1: The proposed rulemaking, draft regulatory guide, and related documents should be issued for public comment.

Staff Response: The staff agrees with the Committee's recommendation.

Committee Recommendation 2: The guidance should be more specific on methods to screen components based on high-level principles as an alternative to a detailed examination of every digital asset. This approach should be discussed with industry during the public comment period and addressed when the final rule and regulatory guide are completed.

Staff Response: The staff agrees that it may be appropriate to include specific methods to screen components based on high-level principles, like defensive architecture, in the subject rule. This type of screening method was not incorporated into the proposed rule because the staff has not observed the deployment of defensive architectures at fuel cycle facilities, except for classified networks. An effective defensive architecture requires consideration of all pathways that potential cyber attacks may exploit (e.g., network, wireless, portable media, and physical access). The staff recognizes that an effective defensive architecture would provide adequate cyber security and acknowledges that incorporating such a screening method into the rule may encourage the future development of effective defensive architectures by fuel cycle licensees.

For situations where an effective defensive architecture cannot be achieved, the proposed rule attempts to minimize the burden through the application of a graded, consequence-based approach to identify and protect vital digital assets (i.e., those digital assets associated with a consequence of concern for which no alternate means of preventing the consequence of concern exists). The proposed rule would require cyber security controls to be addressed only for vital digital assets. Several fuel cycle licensees have indicated that they expect to have few, if any, vital digital assets because they plan to primarily credit alternate means in providing the necessary protection. Also, the draft regulatory guide demonstrates how a licensee can minimize the administrative burden associated with the identification of vital digital assets by using existing documentation and analyses that support current safety and security programs.

For digital assets where alternate means cannot be credited to provide the necessary protection (i.e., vital digital assets), the draft regulatory guide provides methods to minimize the burden of addressing cyber security controls. The draft regulatory guide demonstrates how licensees have the flexibility to designate the boundaries (e.g., network) and group together (e.g., type accreditation) vital digital assets, thereby treating multiple vital digital assets as a single vital digital asset. Additionally, the draft regulatory guide demonstrates how a licensee can minimize administrative burden by: (1) using common or inherited cyber security controls; and (2) simplifying the records (i.e., supporting technical documentation) associated with digital assets, alternate means, and controls. Furthermore, the draft regulatory guide explains how high-level principles (e.g., isolation) may be used to satisfy a number of cyber security controls and thus provide protection against multiple attack vectors. The staff notes that the cyber security controls in the draft regulatory guide were informed by the National Institute of Standards and Technology's (NIST's) special publications, frameworks, and profiles on cyber security. Recent Executive Orders have recommended the NIST approach. The number of cyber security controls are a function of the multiple attack vectors that an effective cyber security program must protect against. The staff tailored NIST's cyber security controls by: (1) selecting only controls relevant to the proposed program performance objectives; (2) organizing control sets applicable to the types of consequences of concern; and (3) establishing graded parameters for controls, suitable to each type of consequence of concern.

Although there has already been extensive outreach to inform development of the proposed rule, the staff agrees with the Committee's recommendation to discuss additional screening methods with stakeholders during the public comment period. Additional stakeholder interactions may provide further information on methods to minimize the regulatory burden. As such, the staff plans to conduct public meetings and workshops to help ensure a shared understanding of the requirements within the proposed rule and an acceptable approach to implement the rule's provisions as described in the draft regulatory guide. The staff is committed to remaining vigilant that the burden to implement the final rule will not grow or become excessive.

We thank the Committee for its expeditious and timely review and look forward to working with the Committee in the future.

Sincerely,

/RA by Frederick D. Brown for/

Victor M. McCree
Executive Director
for Operations

Docket No. NRC-2015-0179

cc: Chairman Svinicki
Commissioner Baran
Commissioner Burns
SECY

DRAFT PROPOSED RULEMAKING 10 CFR 73.53, "REQUIREMENTS FOR CYBER SECURITY AT NUCLEAR FUEL CYCLE FACILITIES," RELATED PARTS 70, 73, AND 40, AND DRAFT REGULATORY GUIDE DG-5062, "CYBER SECURITY PROGRAMS FOR NUCLEAR FUEL CYCLE FACILITIES" DATED: AUGUST 31, 2017

DISTRIBUTION: OEDO-17-00410

RidsEdoMailCenter RidsAcrsAcnw_MailCTR JAndersen, NSIR
JBeardsley, NSIR CPantalo, NSIR CMaupin, NMSS
MBartlett, NMSS

ADAMS ACCESSION NUMBER: ML17180A072 ***via e-mail**

OFC	FCSE/ECB	FCSE/ECB	NMSS/FCSE	NMSS/MSTR
NAME	JDowns	JZimmerman	CErlanger	DCollins
DATE	06/29/2017 07/11/2017 08/09/2017	07/03/2017 07/11/2017 08/10/2017	07/03/2017 07/12/2017 08/10/2017	07/03/2017 07/12/2017
OFC	Tech Ed	NMSS	EDO	
NAME	WMoore	MDapas	VMcCree FBrown for	
DATE	07/05/2017 07/13/2017 08/11/2017*	07/17/2017 08/16/2017 08/30/2017	08/31/2017	

OFFICIAL RECORD COPY