UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

June 21, 2017

Mr. Victor McCree
Executive Director for Operations
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: 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"

Dear Mr. McCree:

During the 644th meeting of the Advisory Committee on Reactor Safeguards, June 7-9, 2017, we completed our review of draft proposed rulemaking 10 CFR 73.53, related Parts 70, 73, and 40, and draft Regulatory Guide DG-5062 in preparation for issue for public comment. Our Digital Instrumentation & Control (DI&C) Systems Subcommittee also reviewed this matter during meetings on November 2, 2016 and February 23, 2017. During these meetings, we had the benefit of discussions with representatives of the NRC staff and input from the Nuclear Energy Institute. We also had the benefit of the referenced documents.

RECOMMENDATIONS

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

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.

BACKGROUND

The purpose of the proposed rule is to amend 10 CFR Part 73, "Physical Protection of Plants and Materials," and related Parts 40 and 70. The associated draft Regulatory Guide DG-5062 is to provide cyber security implementation guidance for the new required cyber security program for certain nuclear fuel cycle facility applicants and licensees.

In the March 24, 2015 staff requirements memorandum for SECY-14-0147, the Commission directed the staff to proceed with a high-priority cyber security rulemaking for fuel cycle facilities (FCFs). In response, the staff prepared the proposed rule and associated draft regulatory guide that would amend the current regulations in 10 CFR Part 73, and make conforming changes to additional regulations in 10 CFR Parts 40 and 70, to establish cyber security requirements for

certain FCF applicants and licensees. The proposed regulation would require FCF applicants and licensees to establish, implement, and maintain a cyber security program designed to promote common defense and security and to provide reasonable assurance that the public health and safety remain adequately protected against the evolving risk of cyber-attacks.

The proposed requirements would apply to each applicant or licensee that is or plans to be authorized to: (1) possess greater than a critical mass of special nuclear material (SNM) and engage in enriched uranium processing, fabrication of uranium fuel or fuel assemblies, uranium enrichment, enriched uranium hexafluoride conversion, plutonium processing, fabrication of mixed-oxide fuel or fuel assemblies, scrap recovery of SNM, or any other FCF activity that the Commission determines could significantly affect public health and safety; or (2) engage in uranium hexafluoride conversion or uranium hexafluoride deconversion.

The proposed revisions to Parts 40 and 70 specify that licensees, current or new, must include in their license a cyber security plan. Changes that decrease the effectiveness of the cyber security plan must be submitted to the Commission for approval. Changes that do not decrease effectiveness can be accomplished without Commission approval, but a report describing the changes must be submitted and a record of the changes must be maintained for three years.

The revisions to Part 73 are administrative with the following two exceptions:

- The proposed revision to 73.46(g)(6) incorporates cyber security programs into the 12-month review requirements already required for physical security

- The proposed new rule 73.53, “Requirements for cyber security at nuclear fuel cycle facilities” requires each licensee (current or applicant) to submit a cyber security plan that satisfies the requirements of this section for Commission review and approval

The rule further identifies requirements for the plan as summarized below:

A. Establishes Program Objectives - The applicant or licensee must establish a cyber security program that will detect, protect against, and respond to a cyber-attack capable of causing one or more of the consequences of concern.

B. Establishes four types of consequences of concern –

(1) **Latent consequences of concern – design basis threat**. The compromise, as a result of a cyber-attack at a facility of a licensee authorized to possess or use a formula quantity of strategic special nuclear material, of a function needed to prevent one or more of the following:
   (i) Radiological sabotage,
   (ii) Theft or diversion of formula quantities of strategic special nuclear material, or
   (iii) Loss of nuclear material control and accounting for strategic special nuclear material.

(2) **Latent consequences of concern – safeguards**. The compromise, as a result of a cyber-attack at a facility of a licensee authorized to possess or use special nuclear material of moderate strategic significance, of a function needed to prevent one or more of the following:
   (i) Unauthorized removal of special nuclear material of moderate strategic significance; or

(ii) Loss of nuclear material control and accounting for special nuclear material of moderate strategic significance.

(3) **Active consequences of concern – safety**. One or more of the following that directly results from a cyber-attack:
   (i) A radiological exposure of 0.25 Sv (25 rem) or greater for any individual;
   (ii) An intake of 30 mg or greater of uranium in soluble form for any individual outside the controlled area; or
   (iii) An acute chemical exposure that could lead to irreversible or other serious, long-lasting health effects for any individual.

(4) **Latent consequences of concern – safety and security**. The compromise, as a result of a cyber-attack, of a function needed to prevent one or more of the following:
   (i) A radiological exposure of 0.25 Sv (25 rem) or greater for any individual;
   (ii) An intake of 30 mg or greater of uranium in soluble form for any individual outside the controlled area; or
   (iii) An acute chemical exposure that could lead to irreversible or other serious, long-lasting health effects for any individual; or
   (iv) Loss or unauthorized disclosure of classified information or classified matter.

C. Requires a cyber security program that establishes a cyber security team, cyber security controls, identifies digital assets whose compromise could result in a consequence of concern, defines a digital asset as vital if no alternate means that is protected from a cyber-attack can be credited to prevent the consequence of concern, ensures that each vital digital asset is protected against a cyber-attack, and identifies temporary compensatory measures when cyber security controls are degraded.

D. Requires a cyber security plan that describes how the program objectives are met.

E. Requires the establishment of a configuration management system.

F. Requires reviews and identifies necessary elements of the reviews for the cyber security program.

G. Requires event reporting and tracking of degradations of controls.

H. Requires records and record retention.

A latent consequence of concern occurs when a digital asset is compromised, but there is no immediate impact on a safety, security, or safeguards function until a secondary event occurs (i.e., an initiating event separate from the cyber-attack).

An active consequence of concern occurs when the compromise of the digital asset directly results in a radiological or chemical exposure exceeding allowable values.

Draft Regulatory Guide DG-5062 describes methods and procedures that the staff considers acceptable for an FCF licensee to use in establishing, implementing, and maintaining a cyber security program subject to the requirements in 10 CFR 73.53.

The draft guide also describes the elements required in a cyber security plan as noted in 73.53 and includes Appendices A through G as follows:

A. Provides a cyber security plan template,

B. Cyber Security Controls for Vital Digital Assets with any Consequence of Concern which is applicable for all types of FCF licensees,

C. Additional Cyber Security Controls for Vital Digital Assets Associated with Latent Consequences of Concern – Design-Basis Threat (Category I Facilities Only),

D. Additional Cyber Security Controls for Vital Digital Assets Associated with Latent Consequences of Concern – Safeguards (Category II Facilities Only),

E. Additional Cyber Security Controls for Vital Digital Assets Associated with Active Consequences of Concern – Safety, which is applicable for all types of FCF licensees,

F. Additional Cyber Security Controls for Vital Digital Assets Associated with Latent Consequences of Concern – Safety and Security, which is applicable for all types of FCF licensees, and

G. Example Identification Process, Alternate Means Analysis, Implementing Procedure, and Additional Considerations.

DISCUSSION

The rule requires FCFs to establish a cyber security program that will detect, protect against, and respond to a cyber-attack capable of causing one or more of the consequences of concern. The objectives are to protect against: radiological sabotage; unauthorized removal, theft, diversion, and loss of material control for SNM; radiological exposure, acute chemical exposure, or ingestion of materials exceeding allowable limits; and loss or unauthorized disclosure of classified information or classified matter.

To meet FCFs performance objectives, the approach for cyber security is control of access (effectively ensuring only authorized access to the digital assets that execute plant processes) and materials control and accountability methods for SNM. In these circumstances, the cyber security threats have two basic sources; those originating external from the plant (for non-isolated internet facing systems) and those initiated internal to the plant.

Regardless of the nature of the plant systems, the proposed rule and the regulatory guide start by requiring identification of all digital assets that, if compromised by a cyber-attack, would result in a consequence of concern. Then, each must be analyzed to determine if it is a vital digital asset by considering whether or not it has an alternate means available that addresses all threat vectors. Those with no alternate means are vital.

The guidance specifies a procedure to screen out components that do not need to be part of the cyber security plan. However, we are concerned that during the implementation phase, the administrative burden will grow and become excessive. Industry has expressed similar concerns. We recommend that the guidance be more specific on methods to screen components based on high-level principles as an alternative to a detailed examination of every digital asset. For example, when defensive architectures are deployed, most of these components may be easily screened out because isolation protects from external cyber threats and configuration management is used to protect against internal threats.

Appendix G provides an example using a simple plant process of how this analysis is executed and the documentation that must be produced and maintained to reach a conclusion that the vital digital asset is adequately protected. The example, even though simple, requires substantial effort to come to an adequacy conclusion. The example uses the detailed approach in the guidance, which examines each digital asset in excruciating detail against dozens of cyber controls with associated documentation and implementing procedures. An additional example should be included that applies a higher-level approach, such as defensive architectures, where boundaries are established that isolate a single asset or dozens of assets against external threats.

The regulatory analysis included examples of recent cyber-attacks that had physical consequences and that illustrate the importance of digital asset isolation from the external world to eliminate external complex cyber-attacks. Isolation as a defensive measure may result in an easier determination of which digital assets are vital and reduce the resources needed to achieve adequate cyber security protections to only internal threats. The proposed DG-5062, Section 6.3.1, was expanded to discuss this concept, yet defensive architectures and isolation from external cyber threats are not identified in the guidance.

An alternative approach using methods to screen components based on high-level principles rather than a detailed examination of every digital asset should be discussed with industry during the public comment period and addressed when the final rule and regulatory guide are completed.

Industry has also expressed concerns with the scope of the proposed rule, but we have not yet discussed this with the staff.

We look forward to working with the staff after the public comment period for the proposed rulemaking.

Sincerely,

/RA/

Dennis C. Bley
Chairman

REFERENCES:

1. U.S. Nuclear Regulatory Commission, “Proposed Rule – Cyber Security at Fuel Cycle Facilities (RIN 3150-AJ64; NRC-2015-0179),” May 1, 2017 (ML17145A327).

2. U.S. Nuclear Regulatory Commission, Draft Regulatory Guide DG-5062, “Cyber Security Programs for Nuclear Fuel Cycle Facilities,” May 2017 (ML17145A340).

3. U.S. Nuclear Regulatory Commission, *Federal Register* Notice, “10 CFR Parts 40, 70, and 73 [NRC-2015-0179] RIN 3150-AJ64, Cyber Security at Fuel Cycle Facilities,” May 1, 2017 (ML17145A342).

4. U.S. Nuclear Regulatory Commission, SRM-SECY-14-0147, “Staff Requirements – SECY-14-0147 – Cyber Security for Fuel Cycle Facilities,” March 14, 2015 (ML15083A175).

5. U.S. Nuclear Regulatory Commission, “Draft Backfit Analysis and Documented Evaluation for Proposed Rule: Cyber Security at Fuel Cycle Facilities (10 CFR 73.53),” May 1, 2017 (ML17145A330).

6. U.S. Nuclear Regulatory Commission, “Draft Regulatory Analysis for Proposed Rule: Cyber Security at Fuel Cycle Facilities (10 CFR Part 73),” May 1, 2017 (ML17145A336).

7. U.S. Nuclear Regulatory Commission, “Draft Environmental Assessment and Finding of No Significant Impact for the Proposed Rule: Cyber Security at Fuel Cycle Facilities,” May 1, 2017 (ML17145A333).

8. (Nuclear Energy Institute), “ACRS Subcommittee Review of the Proposed Fuel Cycle Facility Cyber Security Rulemaking,” October 26, 2016 (ML17166A092).

4. U.S. Nuclear Regulatory Commission, SRM-SECY-14-0147, "Staff Requirements – SECY-14-0147 – Cyber Security for Fuel Cycle Facilities," March 14, 2015 (ML15083A175).

5. U.S. Nuclear Regulatory Commission, "Draft Backfit Analysis and Documented Evaluation for Proposed Rule: Cyber Security at Fuel Cycle Facilities (10 CFR 73.53)," May 1, 2017 (ML17145A330).

6. U.S. Nuclear Regulatory Commission, "Draft Regulatory Analysis for Proposed Rule: Cyber Security at Fuel Cycle Facilities (10 CFR Part 73)," May 1, 2017 (ML17145A336).

7. U.S. Nuclear Regulatory Commission, "Draft Environmental Assessment and Finding of No Significant Impact for the Proposed Rule: Cyber Security at Fuel Cycle Facilities," May 1, 2017 (ML17145A333).

8. (Nuclear Energy Institute), "ACRS Subcommittee Review of the Proposed Fuel Cycle Facility Cyber Security Rulemaking," October 26, 2016 (ML17166A092).

Accession No: ML17171A209 **Publicly Available Y** **Sensitive N**
Viewing Rights: ☒ NRC Users or ☐ ACRS Only or ☐ See Restricted distribution

OFFICE	**ACRS/TSB**	**SUNSI Review**	**ACRS/TSB**	**ACRS**	**ACRS**
NAME	CAntonescu	CAntonescu	MBanks	AVeil	DBley (AV for)
DATE	6/20/17	6/20/17	6/21/17	6/21/17	6/21/17

OFFICIAL RECORD COPY