NIMA ASHKEBOUSSI
Sr. Project Manager, Materials Safety

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

NUCLEAR ENERGY INSTITUTE

June 2, 2016

Mr. Daniel S. Collins, Director
Division of Material Safety, State, Tribal and Rulemaking Programs
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Part 37 Byproduct Materials Cyber Security

Project Number: 689

Dear Mr. Collins:

On behalf of the Nuclear Energy Institute's (NEI)[1] members, I would like to thank you for your letter[2] providing advanced notification of the Nuclear Regulatory Commission's (NRC) intent to distribute a cyber security questionnaire to licensees possessing Category 1 or 2 quantities of radioactive material as defined in 10 CFR Part 37. As requested, NEI notified our members that they might receive a questionnaire related to cyber security of byproduct material and communicated its purpose. We understand that staff is seeking out this data to better understand potential vulnerabilities and risks as described in the SECY-12-0088 cyber security roadmap. As your staff reviews the questionnaire responses, we offer the following additional information and considerations as you evaluate possible future actions.

Power Reactors Implement Strong Cyber Security Programs

If the NRC pursues cyber security rulemaking for byproduct material, it should consider explicitly excluding power reactors that possess this material inside the protected area. Nuclear power reactors have cyber security and physical security attributes (technologically advanced detection, insider mitigation programs and behavior testing) not found in many other critical infrastructure and certainly not found at other NRC licensed facilities. New rulemaking would divert licensee attention and resources from assets that truly require protection.

[1] 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.

[2] April 12, 2016, Letter from Daniel Collins to Nima Ashkeboussi, Notification of Upcoming Distribution of Materials Cyber Security Questionnaire, ML16074A293

Recognizing the lessons of the Part 37 rollout for the power reactors, it would not be prudent to create a similar situation where licensees that are already implementing cyber security regulations under Part 73 are faced with adding new programs that add little value. Since 2002, the nuclear energy industry took the initiative to implement and improve cyber security controls for digital assets needed to maintain nuclear safety and continuity of power well before the NRC mandated regulatory requirements. Additionally, power reactors have expended significant resources implementing the requirements of 10 CFR 73.54 to protect critical digital assets related to safety, security, and control systems. Furthermore, power reactors implement robust physical security programs pursuant to 10 CFR Part 37 and 73. From a risk perspective, radioactive material inside the protected area is secure under Part 73 physical and cyber security programs and additional cyber security regulations would provide little, if any, safety or security benefit while creating unnecessary requirements at a significant cost.

The Scope of the Questionnaire

As your staff evaluates licensee responses to the cyber security questionnaire, we would like to point out that areas of interest in the questions are items that have been considered out of scope for cyber protection in the most recent cyber security proposed rulemaking for fuel cycle facilities (FCF). If rulemaking is considered, we would advise that requirements be focused on protecting assets associated with radiological consequences to the worker and public and not on assets used to maintain security, compliance, or response capabilities. Question 1 focuses on systems that support physical security. In the FCF cyber rulemaking currently underway, the staff is excluding security digital assets for Category III FCF and Part 40 licensees from the scope of the rulemaking. Question 3 focuses on assets used for inventories, data, and records needed for compliance. Generally, licensees are protecting these assets for business purposes. Creating a requirement to protect assets for compliance, and not a safety or security consequence, is not justifiable. Lastly, Question 4 focuses on assets used to support incident response communication. This is being scoped out of the FCF rulemaking due to the diversity of functions and capabilities that are common as well as the unlikelihood that a compromise of a digital asset could prevent a licensee from accomplishing the intended function of communication and event notification. This diversity clearly exists for the wide array of byproduct material licensees.

Consideration of Other Agency Activities

As your staff considers its next steps, we advise a close review of the cyber security efforts undertaken by the Food and Drug Administration in regulating the manufacturers of medical devices that use radioactive materials and the guidance documents they have issued related to cyber security. Furthermore, a majority of Part 37 licensees possessing Category 1 quantities of materials have voluntary security enhancements installed by the National Nuclear Security Administration (NNSA). NNSA evaluated licensee's existing security systems, provided proposed enhancements, funded the installation of new security systems and provided training to security staff and local responders. These security systems are monitored by companies with contracts with NNSA and a full discussion on the cyber protections for these systems should be evaluated with NNSA. These efforts should be adequate to demonstrate operational cyber security for the safety of medical devices and security systems for all licensees with NNSA enhancements.

Utilization of Best Practices Guidance

As NRC evaluated the need for cyber security requirements for non-power reactors, per the SECY-12-0088 cyber security roadmap, the staff came to the conclusion that "cyber security is not currently a risk"[3] for Research and Test Reactors (RTR). We believe that you will come to a similar conclusion that cyber security is not a risk that warrants rulemaking for byproduct material users. In lieu of rulemaking for RTRs, the staff decided to develop a guidance document, "CYBER SECURITY: Effective Practices for the establishment and maintenance of adequate cyber security at Non-Power (Research and Test) Reactor facilities." The document provides consolidated practices and guidance for licensees on understanding cyber security issues and consequences.

Conclusion

There is an extreme variety in the types, sizes, risks, and users of Category 1 and 2 byproduct materials and developing the cyber security requirements that are graded and risk-informed will be complex and challenging. In light of limited NRC and industry resources and the information provided above, it would be prudent for staff to pursue a cyber security "Effective Practices" guide for byproduct materials users, similar to the one issued for RTRs. With minimal effort, the content of the guide can quickly be tailored for implementation to the wide variety of byproduct material users.

We appreciate your consideration of the comments. Please contact me if you have any questions

Sincerely,

Nima Ashkeboussi

Nima Ashkeboussi

c: Ms. Irene Wu, NMSS/MSTR, NRC
Document Control Desk

[3] ML15294A445 - NRC Presentation at the National Organization of Test, Research and Training Reactors 2015 Annual Conference entitled "Effective Practices that Establish Adequate Cyber Security," (10/6/2014)