[7590-01-P]

NUCLEAR REGULATORY COMMISSION

10 CFR Part 37

[NRC-2015-0019]

RIN 3150-AJ56

Cyber Security for Byproduct Materials Licensees

AGENCY: Nuclear Regulatory Commission.

ACTION: Discontinuation of rulemaking activity.

SUMMARY: The U.S. Nuclear Regulatory Commission (NRC) is discontinuing the rulemaking activity that would have developed cyber security requirements for byproduct materials licensees possessing risk-significant quantities of radioactive materials. The purpose of this action is to inform members of the public of the discontinuation of the rulemaking activity and to provide a brief discussion of the NRC's decision. The rulemaking activity will no longer be reported in the NRC's portion of the Unified Agenda of Regulatory and Deregulatory Actions (the Unified Agenda).

DATES: As of May 15, 2018, the rulemaking activity discussed in this document is discontinued.

ADDRESSES: Please refer to Docket ID **NRC-2015-0019** when contacting the NRC about the availability of information regarding this action. You may obtain publicly available information related to this document using any of the following methods:

- **Federal Rulemaking Web site**: Go to http://www.regulations.gov and search for Docket ID **NRC-2015-0019**. Address questions about NRC dockets to Carol Gallagher; telephone: 301-415-3463; e-mail: Carol.Gallagher@nrc.gov. For technical questions, contact the individual listed in the **FOR FURTHER INFORMATION CONTACT** section of this document.

- **NRC's Agencywide Documents Access and Management System (ADAMS)**: You may obtain publicly-available documents online in the ADAMS Public Documents collection at http://www.nrc.gov/reading-rm/ adams.html. To begin the search, select ''ADAMS Public Documents'' and then select "Begin Web-based ADAMS Search." For problems with ADAMS, please contact the NRC's Public Document Room (PDR) reference staff at 1-800-397-4209, 301-415-4737, or by e-mail to pdr.resource@nrc.gov. The ADAMS accession number for each document referenced (if it is available in ADAMS) is provided the first time that it is mentioned in the SUPPLEMENTARY INFORMATION section.

- **NRC's PDR**: You may examine and purchase copies of public documents at the NRC's PDR, Room O1F21, One White Flint North, 11555 Rockville Pike, Rockville, Maryland 20852.

FOR FURTHER INFORMATION CONTACT: Vanessa Cox, Office of Nuclear Material Safety and Safeguards, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001; telephone: 301-415-8342; e-mail: Vanessa.Cox@nrc.gov.

SUPPLEMENTARY INFORMATION:

I. Discussion

The NRC and Agreement States are responsible for overseeing and implementing the National Materials Program to enable the safe and secure use of radioactive materials licensed for commercial, industrial, academic, and medical uses. The program includes thousands of byproduct materials licensees in varying operating environments, ranging from small industrial radiography and well-logging businesses to large manufacturing facilities, universities, and medical facilities. The majority of the licensees that possess risk-significant quantities of radioactive materials are regulated by Agreement States. Risk-significant quantities of radioactive material are defined as those meeting the thresholds for Category 1 and Category 2 included in appendix A to part 37 of title 10 of the *Code of Federal Regulations* (10 CFR), "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material."

In a Commission paper, SECY-12-0088, "The Nuclear Regulatory Commission Cyber Security Roadmap," dated June 25, 2012 (ADAMS Accession No. ML12135A050), the NRC staff described its plan to evaluate the need for cyber security requirements for NRC and Agreement State licensees and facilities, including byproduct materials licensees. As described in that paper, the NRC staff planned to form a working group, with Agreement State participation, to develop self-assessment tools for licensees and conduct a limited number of site visits. Based on the results of these assessments and site visits, the working group intended to prepare a paper outlining potential actions for Commission consideration.

In July 2013, the NRC established the Byproduct Materials Cyber Security Working Group, comprised of headquarters and regional NRC staff and representation from the Organization of Agreement States. The purpose of the working group was to identify potential cyber security vulnerabilities among commercial, medical, industrial, and academic users of risk-significant radioactive materials and determine if the results warranted regulatory action. The working group worked with the NRC's Intelligence

Liaison and Threat Assessment Branch, which regularly monitors the threats associated with cyber security and shares cyber threat information with licensees, as appropriate.

The working group identified four sets of digital assets that the NRC should evaluate with respect to cyber threat protection:

1) Digital/microprocessor-based systems and devices that support the physical security of the licensee's facilities. These include access control systems, physical intrusion detection and alarm systems, video camera monitoring systems, digital video recorders, door alarms, motion sensors, keycard readers, and biometric scanners;

2) Equipment and devices with software-based control, operation, and automation features, such as panoramic irradiators and gamma knives;

3) Computers and systems used to maintain source inventories, audit data, and records necessary for compliance with security requirements and regulations; and

4) Digital technology used to support incident response communications and coordination such as digital packet radio systems, digital repeater stations, and digital trunk radio systems.

On January 6, 2016, the NRC staff submitted a memorandum to the Commission titled "Staff Activities Related to the Evaluation of Materials Cyber Security Vulnerabilities" (ADAMS Accession No. ML15201A509). This memorandum informed the Commission of the ongoing evaluation to determine the cyber security risk to each of the four sets of digital assets for risk-significant radioactive materials licensees, and described the two-pronged approach focused on information gathering and consequence analysis that was used.

As part of the information gathering effort, the NRC staff distributed a voluntary survey, "Questionnaire on Cyber Security at Byproduct Materials Licensees" (ADAMS Accession No. ML15246A306) on April 29, 2016, to all NRC and Agreement State licensees that possessed Category 1 and 2 quantities of radioactive materials. The

purpose of the questionnaire was to identify what key digital assets existed at each licensee type, how they were connected to internal/external networks and the Internet, and what technical and procedural security measures were in place for protection and operation of these systems and devices. The NRC staff also conducted outreach to stakeholders to encourage completion of the questionnaire, and site visits to manufacturers and panoramic irradiator licensees.

The consequence analysis was conducted in parallel with the information gathering effort, and evaluated the potential for onsite and offsite consequences that could occur if the availability, integrity, or confidentiality of data or systems associated with nuclear materials were compromised by a cyber attack.

Given the regulatory responsibilities of the U.S. Food and Drug Administration (FDA), the NRC limited its evaluation of the software systems used in medical applications to the systems related to the radiation safety and physical protection authority of the NRC. The NRC has a memorandum of understanding with the FDA that clarifies the respective roles of each agency in regulating the safe use of radiopharmaceuticals and sealed sources, and other medical devices containing radioactive material (ADAMS Accession No. ML023520399). Additional information on the FDA's activities, role, and expectations for the continued cyber security of medical devices can be found at https://www.fda.gov/downloads/medicaldevices/digitalhealth/ucm544684.pdf.

On February 28, 2017, the NRC staff provided an update to the Commission on the status of agency activities pertaining to cyber security at licensee facilities in a Commission paper, SECY-17-0034, "Update to the U.S. Nuclear Regulatory Commission Cyber Security Roadmap" (ADAMS Accession No. ML16354A258). The update noted the NRC staff's further consideration of cyber security requirements for radioactive materials licensees since the January 2016 memorandum. Additionally, the

paper stated that the working group planned to complete its evaluation of the questionnaire responses, consequence analysis, and any follow-up communication with stakeholders and develop recommendations for a path forward.

Subsequently, the NRC completed its evaluation of cyber security requirements for byproduct materials licensees in October 2017.

The NRC staff concluded that byproduct materials licensees that possess risk-significant quantities of radioactive material do not rely solely on digital assets to ensure safety or physical protection. Rather, these licensees generally use a combination of measures, such as doors, locks, barriers, human resources, and operational processes, to ensure security, which reflects a defense-in-depth approach to physical protection and safety. As a result, the staff concluded that a compromise of any of the digital assets identified in the January 6, 2016, Commission memorandum would not result in a direct dispersal of risk-significant quantities of radioactive material, or exposure of individuals to radiation, without a concurrent and targeted breach of the physical protection measures in force for these licensees.

Therefore, the NRC staff determined that the current cyber security threat and potential consequences do not warrant regulatory action. However, the NRC staff determined that it would be prudent to issue an Information Notice (IN) to communicate effective practices for cyber security to byproduct materials licensees possessing risk-significant quantities of radioactive material. The IN will provide licensees with a better understanding of contemporary cyber security issues and strategies to protect digital assets (*e.g.*, computers, digital alarm systems), including those used to facilitate compliance with physical security requirements, such as those in 10 CFR part 37. The IN, which will reference existing cyber security guidance developed by the NRC's Office of Nuclear Reactor Regulation and other Federal agencies, will be issued later in 2018.

II. Conclusion

For the reasons discussed in this document, the NRC is discontinuing rulemaking activity to develop cyber security requirements for byproduct materials licensees possessing risk-significant quantities of radioactive materials. In the next edition of the Unified Agenda, the NRC will update the entry for this rulemaking activity and refer to this document to indicate that the rulemaking has been discontinued. This rulemaking activity will appear in the "Completed Actions" section of the next edition of the Unified Agenda, but will not appear in future editions. If the NRC decides to pursue similar or related rulemaking activities in the future, it will inform the public through a new rulemaking entry in the Unified Agenda.

Dated at Rockville, Maryland, this 10th day of May, 2018.

For the Nuclear Regulatory Commission.

/RA/

Victor McCree,
Executive Director for Operations.