UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

January 6, 2016

MEMORANDUM TO: Chairman Burns
Commissioner Svinicki
Commissioner Ostendorff
Commissioner Baran

FROM: Scott W. Moore, Acting Director
Office of Nuclear Material Safety and Safeguards ***/RA/***

SUBJECT: STAFF ACTIVITIES RELATED TO THE EVALUATION OF MATERIALS CYBER SECURITY VULNERABILITIES

The purpose of this memorandum is to inform the Commission of the staff's activities for evaluating the need for cyber security requirements for category 1 and 2 nuclear materials licensees. This memorandum summarizes the operating and regulatory landscape of materials licensees and outlines the actions that the staff is taking to develop potential regulatory actions to manage the risk to information and digital systems for materials licensees.

In SECY-12-0088, "The Nuclear Regulatory Commission Cyber Security Roadmap," (Roadmap) dated June 25, 2012, the staff included a plan to evaluate the need for cyber security requirements for nuclear materials licensees. The paper discussed plans to form a working group, with Agreement State participation, to focus on developing self-assessment tools to gather information on a representative sample of materials licensees. Based on the results of those assessments and a limited number of site visits, the working group will prepare a paper outlining actions for Commission consideration.

In addition, a new recommendation was added in the 2014 Radiation Source Protection and Security Task Force Report for U.S. Government agencies to assess the adequacy of, and coordinate strategies for, preventing and mitigating cybersecurity vulnerabilities related to category 1 and 2 radioactive sources. The new recommendation aligns with Roadmap activities in this area.

The U.S. Nuclear Regulatory Commission (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 increased use of digital technology in devices containing these materials, and associated facilities, could introduce vulnerabilities to cyber threats. In fulfilling their responsibilities, the NRC and Agreement States must understand the extent to which these vulnerabilities, if

CONTACT: Irene Y. Wu, NMSS/MSTR
(301) 415-1951

exploited, could result in an adverse impact on the safety, security, and emergency preparedness of these facilities.

Operating and Regulatory Landscape of Materials Licensees

The cyber security landscape for materials licensees is complex, and presents multiple potential risks, including over 1,000 licensees in a variety of different operating environments. Materials licensees operate in environments ranging from large manufacturing facilities, universities, and medical facilities to small industrial radiography and well logging businesses. Additionally, a majority of the licensees that possess risk-significant quantities of radioactive materials (category 1 and 2) are regulated by Agreement States.

Another consideration is the role of the U.S. Food and Drug Administration (FDA) in regulating the manufacturers of medical devices containing radioactive materials. The NRC has a memorandum of understanding (MOU) with the FDA, which clarifies the respective roles of each agency in regulating the safe use of radiopharmaceuticals and sealed sources, and other medical devices containing radioactive material (available at Agencywide Documents Access and Management System [ADAMS] Accession No. ML023520399). The MOU provides for cooperation between the two agencies and for more effective exchanges of information.

Materials Cyber Security Working Group

The NRC established the Materials Cyber Security Working Group in July 2013 with staff from the Office of Nuclear Material Safety and Safeguards (NMSS), Office of Nuclear Security and Incident Response (NSIR), Office of the General Counsel, Region I, Region III, Region IV, and the Organization of Agreement States. The purpose of the working group is to identify potential cyber security vulnerabilities among commercial, medical, industrial, and academic users of risk-significant radioactive materials and propose regulatory action. The working group works in parallel with the NSIR's Intelligence Liaison and Threat Assessment Branch who regularly monitors the threats associated with cyber security, including potential threats against licensed facilities, and shares cyber threat information through numerous mechanisms, including bi-weekly threat briefings, periodic finished intelligence products, and an annual assessment which includes non-kinetic threats (i.e., cyber-enabled attack that may or may not result in physical damage depending on intent of sponsor and/or unintended consequences).

The working group identified four sets of digital assets that may need protection from cyber threats:

1) Digital/microprocessor-based systems and devices that support the physical security of the licensee's facilities. This includes 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, gamma knives, and fixed radiography.

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

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

To determine the cyber security risk to each of the above focus areas for each category of licensee, the working group is using a two-pronged approach, focusing on information gathering and consequence analysis.

Information Gathering

The information gathering stage of the materials cyber security assessment involves multiple steps, including distribution of a voluntary questionnaire, site visits, and stakeholder outreach, some of which have already been completed. In February 2014, the working group distributed a voluntary questionnaire to a representative cross-section of category 1 and 2 NRC licensees. The results from that initial questionnaire helped to revise the questionnaire to be disseminated to all of the NRC and Agreement State materials licensees that possess category 1 and 2 quantities of radioactive materials. The working group obtained approval from the Office of Management and Budget (OMB) on the questionnaire in April 2015 and plans to distribute the questionnaire to all of the NRC and Agreement State materials licensees that possess category 1 and 2 quantities of radioactive materials. The purpose of the questionnaire is to identify what key digital systems exist at each licensee type, how they are connected to internal/external networks and the internet, and identify the technical and procedural security measures in place for protection and operation of these systems and devices. This information will allow the working group to screen out unrealistic and unreasonable scenarios and consequences, and will allow the working group to identify potential vulnerabilities for further consideration. This information will support the consequence analysis discussed below. The OMB-approved questionnaire is available at ADAMS Accession No. ML15246A306.

The working group has also conducted information gathering visits to two manufacturers and two panoramic irradiator licensees to observe what digital systems are present and how they interface to other systems, both internally and externally. Follow-up site visits and/or conference calls based on responses to the questionnaire may also be warranted.

Throughout the information gathering stage, the working group will conduct outreach to stakeholders to encourage participation with the voluntary questionnaire. The following are some outreach activities that are planned before and after deployment of the questionnaire:

- Continue to keep the Agreement States informed of NRC's materials cyber security efforts through existing methods of communication such as the monthly teleconferences and State and Tribal Communications Letters.

- Engage the FDA within the context of the existing MOU to share information on NRC's materials cyber security efforts and determine what actions FDA is taking with regard to cyber security.

- Provide updates on NRC's materials cyber security efforts to the Radiation Source Protection and Security Task Force.

- Inform licensees of the questionnaire through an article in the NMSS licensee newsletter, and letters to various industry groups.

Consequence Analysis

In parallel with the information gathering effort, the working group is evaluating the potential for onsite and offsite consequences that may occur if the availability, integrity, or confidentiality of data or systems associated with nuclear materials were compromised by a cyber-attack. In some cases, those impacts may have already been considered as part of the Title 10 of the *Code of Federal Regulations* Part 37 vulnerability assessment. The working group is developing a matrix, by licensee type, with potential impacts to each of the four sets of digital assets listed above that may need protection from cyber threats. The working group's consequence analysis will also consider whether any licensees are critical infrastructure, as well as potential impacts from denial of service.

Moving Forward

Following the survey, the working group will complete its evaluation of the questionnaire responses and conduct any follow-up site visits or conference calls by late 2016. The working group will develop recommendations for a path forward to the Commission in early 2017. The recommendations to the Commission will be based on consideration of the threat, credible scenarios, and consequences. Based upon low impacts and low probability of incidence, the working group expects to exclude the need for future action for some materials licensee types altogether, focusing on those for which further regulatory action, such as guidance or rulemaking, may be appropriate. The paper to the Commission will document the bases for proposed future actions.

Throughout this process the working group members will continue to keep various affected stakeholders, including industry and professional organizations, informed of its efforts.

cc: SECY
OGC
OCA
OPA
OCFO

- Provide updates on NRC's materials cyber security efforts to the Radiation Source Protection and Security Task Force.

- Inform licensees of the questionnaire through an article in the NMSS licensee newsletter, and letters to various industry groups.

Consequence Analysis

In parallel with the information gathering effort, the working group is evaluating the potential for onsite and offsite consequences that may occur if the availability, integrity, or confidentiality of data or systems associated with nuclear materials were compromised by a cyber-attack. In some cases, those impacts may have already been considered as part of the Title 10 of the *Code of Federal Regulations* Part 37 vulnerability assessment. The working group is developing a matrix, by licensee type, with potential impacts to each of the four sets of digital assets listed above that may need protection from cyber threats. The working group's consequence analysis will also consider whether any licensees are critical infrastructure, as well as potential impacts from denial of service.

Moving Forward

Following the survey, the working group will complete its evaluation of the questionnaire responses and conduct any follow-up site visits or conference calls by late 2016. The working group will develop recommendations for a path forward to the Commission in early 2017. The recommendations to the Commission will be based on consideration of the threat, credible scenarios, and consequences. Based upon low impacts and low probability of incidence, the working group expects to exclude the need for future action for some materials licensee types altogether, focusing on those for which further regulatory action, such as guidance or rulemaking, may be appropriate. The paper to the Commission will document the bases for proposed future actions.

Throughout this process the working group members will continue to keep various affected stakeholders, including industry and professional organizations, informed of its efforts.

cc: SECY
OGC
OCA
OPA
OCFO

DISTRIBUTION:
RidsEdoMailCenter RidsSecyCorrespondenceMailCenter

ML15201A509

OFC	MSTR	MSTR	MSTR	NMSS/MSTR
NAME	IWu	Via e-mail EQuinones	AGiantelli	JPiccone
DATE	7/21/15	7/20/15	7/29/15	8/04/15
OFC	NSIR/CSD	OGC	TechEd	NMSS
NAME	BWestreich	Via e-mail AGendelman	CPoland	SMoore
DATE	8/21/15	9/04/15	11/25/15	1/6/16

OFFICIAL RECORD COPY