BYPRODUCT MATERIALS CYBERSECURITY WORKING GROUP

CHARTER

PURPOSE

The purpose of the working group (WG) is to identify potential cybersecurity vulnerabilities among commercial, medical, industrial, and academic users of risk significant radioactive materials (Category 1 and Category 2 quantities of radioactive material[1]). The WG will determine if potential cyber threats to information systems or control systems of devices containing risk significant radioactive materials warrant enhanced protection from cyberattacks. The WG's evaluations and recommendation(s) will be documented in a notation vote paper to be completed in September 2017, which will be provided to the Commission.

BACKGROUND

Shortly after the terrorist attacks of September 11, 2001, the U.S. Nuclear Regulatory Commission (NRC) issued a series of orders to its nuclear power plant licensees as well as to risk significant radioactive materials licensees to enhance their overall security. However, the orders issued to nuclear power plant licensees also included specific requirements for addressing certain cybersecurity threats and vulnerabilities and added cyberattacks to the adversary threat types the nuclear power plants must be able to defend against.

As the NRC continued to focus on its priority of imposing physical security requirements on risk significant radioactive materials licensees, for nuclear power plant licensees and applicants, which could be of a greater impact and resultant consequence from a cyberattack, the NRC issued a new cybersecurity rule in March 2009. This new rule, Title 10 *Code of Federal Regulations* (10 CFR) 73.54, "Protection of Digital Computer and Communications Systems and Networks," affected existing nuclear power plant licensees and applicants. The new regulation requires licensees to submit a cybersecurity plan and an implementation schedule for NRC approval.

Following the cybersecurity efforts initiated for nuclear power plant licensees and the increased emphasis on critical infrastructure cybersecurity and preparedness, the NRC, in a graded approach based on risk significance, also considered the need for similar cybersecurity requirements for fuel cycle facilities, spent fuel storage facilities, non-power reactors, decommissioned nuclear facilities, and risk significant radioactive materials licensees.

In alignment with SECY-12-0088, "The Nuclear Regulatory Commission Cyber Security Roadmap," (Roadmap) dated June 25, 2012 (Agencywide Document and Management System (ADAMS) Accession No. ML12135A050), the NRC staff formed the WG in July 2013 as part of the process of evaluating the need for cybersecurity-related regulatory requirements and/or guidance. The WG includes members from the Office of Nuclear Material Safety and Safeguards (NMSS), Office of Nuclear Security and Incident Response (NSIR), Office of

[1] The Category 1 and Category 2 thresholds are based on the quantities established by the International Atomic Energy Agency in its "Code of Conduct on the Safety and Security of Radioactive Sources," which the United States has committed to, and the NRC has endorsed. Category 1 and Category 2 quantities of radioactive material are considered risk significant and are listed in Table A-1 of Appendix A, "Category 1 and Category 2 Radioactive Materials," to 10 CFR Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material."

General Counsel, Region I, Region III, Region IV, and an Organization of Agreement State representative.

A new recommendation was subsequently added to the 2014 Radiation Source Protection and Security Task Force Report which was submitted to the President and Congress (ADAMS Accession No. ML14153A182) 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 recommendation aligns with and tracks the status of progress being made in regard to the WG. Also, on January 6, 2016, a memo was issued to the Commission (ADAMS Accession No. ML15201A509) to inform the Commission of the actions that the staff is taking to develop any regulatory measures or guidance to manage the risk to information and digital systems for radioactive materials licensees.

WORKING GROUP AND STEERING COMMITTEE MEMBERSHIP

The WG and Steering Committee (SC) will function as an NRC internal WG with Agreement State participation in accordance with Management Directive 5.3, "Agreement State Participation in Working Groups." The WG will be chaired by an NRC staff member and the SC will be chaired by a representative from NRC management.

U.S Nuclear Regulatory Commission/Agreement State Working Group and Steering Committee
Byproduct Materials Cybersecurity

Organization	Working Group	Steering Committee
Office of Nuclear Material Safety and Safeguards (NMSS)	Kim Lukes, Chair Margaret Cervera Ernesto Quinones	Daniel Collins, Director, Division of Material Safety, State, Tribal, and Rulemaking Programs
Office of Nuclear Security and Incident Response (NSIR)	Charity Pantalo Gary Purdy	James Andersen, Director, Division of Physical and Cyber Security Policy
Office of the General Counsel	John Hull Lorraine Baer	Carrie Safford, Assistant General Counsel for High-Level Waste, Fuel Cycle, and Nuclear Security
Region I	Michael Reichard	James Trapp, Director, Division of Nuclear Materials Safety, Region I
Region III	Geoffrey Warren	
Region IV	Michael Vasquez	
Agreement State	Brian Goretzki (AZ)	TBD

Other Resource Representatives: Representatives from the Computer Security Office, Office of Information Services, and Office of Nuclear Reactor Regulation may be invited to participate in certain WG activities requiring special expertise. Other NMSS staff members may contribute to the WG as resources. Contract support with cybersecurity-related expertise will serve in a consultation capacity. Coordination with other agencies such as U.S. Department of Energy, specifically, National Nuclear Security Administration, the Federal Bureau of Investigation, the Food and Drug Administration, and the Department of Homeland Security may be conducted, as appropriate.

If the WG concludes that enhancements be made to 10 CFR Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material," and/or guidance (such as enhancements to existing guidance documents ("Implementation Guidance for 10 CFR Part 37, Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material" (NUREG-2155) and/or "Physical Security Best Practices for the Protection of Risk-Significant Radioactive Material" (NUREG-2166)), these proposals will be provided to the appropriate working group for disposition as either rulemaking and/or guidance changes.

ACTIVITIES

The WG will assess a representative cross-section of risk significant radioactive materials licensees to better understand the potential vulnerabilities and risks associated with cyber threats.

The assessment will focus, at a minimum, on the following tasks:

1. Identify key digital assets to be protected from cyber threats, focusing on:
    - 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.
    - Equipment and devices with software-based control, operation, and automation features, such as panoramic irradiators and stereotactic radiosurgery units.
    - Computer/systems used to maintain source inventories, audit data, and records necessary for compliance with security requirements and regulations.
    - Digital technology used to support incident response communications/coordination such as digital packet radio systems, digital repeater stations, and digital trunk radio systems.
2. Determine what key digital systems and devices exist at each licensee type.
3. Determine how systems and devices are connected to internal and external networks, and the internet.
4. Identify the technical and procedural security measures in place for protection and operation of these systems and devices and assess potential vulnerabilities.
5. Identify the potential consequences that may occur from loss of control, or if the availability, integrity, or confidentiality of the data contained in the system were compromised.

The results of the WG's assessment will be used as input to the Commission notation vote paper. The WG will meet with the SC to obtain endorsement of the results of their assessment and the options and recommendation(s) that will be provided in the Commission notation vote paper.

SCHEDULE

The WG will complete its assessment by Summer 2017. The Commission notation vote paper is to be provided to the Office of the Executive Director of Operations on September 29, 2017.

LEVEL OF EFFORT EXPECTED OF PARTICIPANTS

The WG will meet for 1 to 2 hours on a monthly to bimonthly basis. Between meetings, WG members should expect to spend an additional 2 to 4 hours reviewing relevant documents and developing content for the assessment tools and the Commission notation vote paper. WG members should expect to attend the SC meetings (anticipated to be approximately two SC meetings) and the periodic briefings with interested managers on the WG activities or contents of the Commission notation vote paper to solicit feedback and comments.

The NRC staff should charge hours expended for this effort to CAC A34004 (Generic Homeland Security).

MEETINGS

Meetings are pre-decisional and will be closed to the public.

WG members may delegate an alternative representative for a specific meeting. The WG may also invite individual(s) to a meeting to participate as a resource to assist the WG. However, the Chair or designee must be present during any WG meetings.

There are several forms of media that will be made available for maximum use to facilitate the interactions between WG members (e.g., conference calls, Go-To-Meeting, and electronic mail). The meetings will generally be held in the Washington, D.C. area, unless alternate locations are agreed upon by WG members. If travel is necessary, travel and per diem expenses for Agreement State members of the WG will be covered by the Division of Material Safety, State, Tribal, and Rulemaking Programs. Regions are responsible for the travel expenses of their staff.

APPROVED

/RA/ May 15, 2017

Daniel S. Collins, Nuclear Regulatory Commission Date

SUBJECT: BYPRODUCT MATERIALS CYBERSECURITY WORKING GROUP CHARTER

ML17110A114

OFC	NMSS/MSTR	NMSS/MSTR	NMSS/MSTR
NAME	KLukes	DWhite	DCollins
DATE	05/4/2017	05/15/2017	05/15/2017

OFFICIAL RECORD COPY