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

April 12, 2016

ALL AGREEMENT STATES, WYOMING, VERMONT

NOTIFICATION OF UPCOMING DISTRIBUTION OF MATERIALS CYBER SECURITY QUESTIONNAIRE (STC-16-034)

Purpose: To announce upcoming distribution of a cyber security questionnaire to U.S. Nuclear Regulatory Commission (NRC) and Agreement State licensees who possess Category 1 and 2 radioactive material.

Background: The NRC formed the Byproduct Materials Cyber Security Working Group to focus on identifying potential cyber security vulnerabilities among medical, industrial, and academic users of risk-significant radioactive materials. This working group is comprised of staff from the NRC's Offices of Nuclear Material Safety and Safeguards, Nuclear Security and Incident Response; and Regions I, III, and IV, as well as an Agreement State representative.

The NRC recently documented the status of staff activities related to the evaluation of materials cyber security vulnerabilities in a memorandum to the Commission dated January 6, 2016, which can be found in the NRC's Agencywide Documents Access and Management System (ADAMS) under Accession No. ML15201A509.

Discussion:

In the near future, the working group will be distributing a questionnaire to all NRC and Agreement State byproduct materials licensees that possess Category 1 or 2 radioactive materials. Licensees will receive the questionnaire by e-mail from MaterialsCyber.Resource@nrc.gov. In the e-mail, licensees will be provided guidance on what information should not be included in their response and instructions on how to submit responses to the questionnaire. As discussed on the March 17, 2016, conference call with the Organization of Agreement States and the Conference of Radiation Control Program Directors, the NRC will distribute the questionnaire using the e-mail addresses in both the National Source Tracking System and the Web-Based Licensing System. Licensees are not required to respond to the questionnaire; however, a response would be greatly appreciated as it will help the working group better understand the potential vulnerabilities and risks associated with cyber threats, and will help form the basis for any recommendations and possible actions for consideration.

The questionnaire covers, but is not limited to, the following areas:

- The use of devices with software-based control systems, such as irradiators and stereotactic radiosurgery systems.
- The use of access control or intrusion detection systems that support the physical security of facilities.
- The use of computer systems that licensees use to maintain their source inventories and security records.
- The use of digital technology to support response communications/coordination.

A copy of the questionnaire to be distributed is attached. The NRC is requesting that responses to these questionnaires be submitted within 30 days from receipt of the e-mail. Based on the responses received, follow-up conference calls and/or site visits may be requested. The working group will coordinate with Agreement State staff when following up with Agreement State licensees.

If you have any questions regarding this correspondence, please contact me at (301) 415-3340 or the individual named below:

POINT OF CONTACT: Irene Wu E-MAIL: Irene.Wu@nrc.gov
TELEPHONE: (301) 415-1951

/RA/

Daniel S. Collins, Director
Division of Material Safety, State, Tribal
and Rulemaking Programs
Office of Nuclear Material Safety
and Safeguards

Enclosure:
Materials Cyber Security Questionnaire

Approved by OMB: No. 3150-0227 Expires: 04/30/2018

Submit responses to MaterialsCyber.resource@nrc.gov.

Questionnaire on Cyber Security at Byproduct Materials Licensees

In order to aid the NRC in evaluating cyber security at byproduct materials licensees, it would be helpful if you responded to the following questions. Responses to these questions are not required, and no adverse action will result from not responding to this survey or from any responses to this survey. Please do not include any Safeguards Information or other controlled information in your responses.

Date:
Name:
Company Name:
License Number(s):
Phone Number:
Email Address:
License Category (select one): Academic, Disposer, Distributor, Fuel Cycle Facility, Irradiator, Medical, Power Reactor, Radiography, Research Reactor, Research and Development, Waste Broker, Well Logging, Other

1. Digital/microprocessor-based systems and devices that support the physical security of licensee 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, biometric scanners, etc:

    - Does the facility have a digital access monitoring and control system? [Yes]/[No]
    - Does the facility have a digital intrusion detection/alarm system? [Yes]/[No]
    - Does the facility have a digital video monitoring/surveillance system? [Yes]/[No]
    - Are any such systems connected to a facility local area network? [Yes]/[No]
    - Is the facility local area network connected/bridged into any other network? [Yes]/[No]
    - Can any of these systems be remotely accessed by the vendor? [Yes]/[No]
    - Can any of these computers be remotely accessed by the IT organization? [Yes]/[No]
    - Are any of these systems remotely monitored for incident response? [Yes]/[No]
    - Do any of these systems employ wireless technology? [Yes]/[No]
    - Is the maintenance/support of any of these systems outsourced? [Yes]/[No]
    - Is portable media used to move data/files to or from any of these systems? [Yes]/[No]
    - If you would like to elaborate on any of your above answers, please use the space below.

Enclosure

2. Devices/equipment with software-based control, operation, and automation features, such as panoramic irradiators, gamma knives, and fixed radiography:

    - Are any of these devices connected to a facility local area network? [Yes]/[No]
    - Is the facility local area network connected/bridged into any other network? [Yes]/[No]
    - Can any of these devices be remotely accessed by the vendor? [Yes]/[No]
    - Can any of these computers be remotely accessed by the IT organization? [Yes]/[No]
    - Are any of these devices remotely monitored for incident response? [Yes]/[No]
    - Do any of these devices employ wireless technology? [Yes]/[No]
    - Is maintenance/support of any of these devices outsourced? [Yes]/[No]
    - Is portable media used to move data/files to or from any of these devices? [Yes]/[No]
    - Are periodic/occasional updates made to the software of any of these devices? [Yes]/[No]
    - If you would like to elaborate on any of your above answers, please use the space below.

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

    - Are any of these computers connected to a facility local area network? [Yes]/[No]
    - Is the facility local area network connected/bridged into any other network? [Yes]/[No]
    - Can any of these computers be remotely accessed by the vendor? [Yes]/[No]
    - Can any of these computers be remotely accessed by the IT organization? [Yes]/[No]
    - Do any of these computers employ wireless technology? [Yes]/[No]
    - Is maintenance/support of any of these computers outsourced? [Yes]/[No]
    - Is portable media used to move data/files to or from any of these computers? [Yes]/[No]
    - Are periodic/occasional updates made to the software on any of these computers? [Yes]/[No]
    - Is any form of encryption used to protect sensitive data on these computers? [Yes]/[No]
    - Are these computers given the latest security patches on a regular basis? [Yes]/[No]
    - Do any of these computers support email or web browsing functions? [Yes]/[No]
    - If you would like to elaborate on any of your above answers, please use the space below.

4. Digital technology used to support incident response communications/coordination such as a digital packet radio system, digital repeater stations, digital trunk radio, etc:

    - Are all such systems and associated components tested on a periodic basis? [Yes]/[No]
    - Are all portable components of such systems periodically inspected for tampering? [Yes]/[No]
    - Are all stationary components of such systems located in physically secure areas? [Yes]/[No]
    - Have any radio system components received software upgrades from the vendor? [Yes]/[No]
    - Is radio system provisioning (changes) performed by licensee personnel? [Yes]/[No]
    - If you would like to elaborate on any of your above answers, please use the space below.