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 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, 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.

2. Devices 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.