IMPLEMENTING GUIDANCE FOR LICENSEES THAT
POSSESS RADIOACTIVE MATERIAL QUANTITIES OF CONCERN

Access Control

The objective is to limit "access" to radioactive material quantities of concern and devices containing radioactive material quantities of concern (devices) so that the risk of theft, sabotage, or unauthorized use is minimized. Access means that an individual could exercise some physical control over the material or device. These access control requirements supplement existing regulations that address security and control of radioactive material by further limiting unescorted access to only those individuals approved by the licensee.

If access to radioactive material quantities of concern or the device is required by an individual who has not been approved for unescorted access, the non-approved individual must be escorted by an approved individual. Escorting means maintaining line of sight with the escorted individual. Licensees should also establish a means by which individuals approved for unescorted access can be visually distinguished from those requiring escort. For example, those approved for unescorted access to radioactive material quantities of concern or the device could wear specially colored badges or other identifying articles. This may assist facility personnel in early detection of unauthorized access to radioactive material quantities of concern or the device.

Control of access to radioactive material quantities of concern and the device can be achieved by the following examples:

Limiting distribution of keys, keycards, or combinations to doors and gates to approved individuals;
Remote activation of locked doors and gates using remote surveillance;
Using a card reader and electronic locking devices at control points; and
Constant surveillance by a person approved for unescorted access.

These requirements also apply at temporary job sites. Additionally, when transporting radioactive material quantities of concern, including the device, to and from a temporary jobsite,

access control shall be maintained when the transport vehicle is stopped at a hotel, restaurant, gas station, or other location.

Detection and Assessment

The licensee shall have a documented program to immediately detect unauthorized access to material when it occurs, assess whether the unauthorized access was an actual or attempted theft, and if so, initiate appropriate response. The objective is to reduce the risk that the material will be stolen and used for unauthorized purposes, and improve the opportunity for recovery if stolen.

In order to facilitate the immediate detection, assessment and response, the radioactive material quantities of concern and devices containing such material shall be monitored to detect unauthorized access. Monitoring may be accomplished by a variety of means, including:

- a monitored intrusion alarm (an intrusion detection system with the capability to detect unauthorized access and that is linked to an on-site or off-site central monitoring facility);
- electronic devices for intrusion detection (alarms that will alert nearby facility personnel); or
- visual monitoring (video surveillance cameras, and/or visual inspection by trained personnel).

Systems used to control access to high radiation areas as required by 10 CFR Part 20, or equivalent Agreement State Regulations, or other detection and access control systems used for radiation protection may be used or modified, provided the modifications do not compromise the original safety purpose. Documentation should describe how these systems provide the required intrusion detection.

The licensee is responsible for enhanced monitoring during source delivery and shipment when the delivery or shipment exceeds 100 times the Table 1 values. Some examples of enhanced monitoring are providing additional personnel to monitor the radioactive material or increasing video surveillance of the radioactive material. When a service provider takes temporary possession of a source at a licensed facility, during these activities, the licensee, not the service provider, is responsible for the enhanced monitoring as well as the other requirements.

The licensee shall establish a program for assessing and responding to unauthorized access so that prompt mitigating measures can begin. Assessment can be by either automated devices or trained personnel who can initiate the appropriate response. Licensees should consider the possibility of simultaneous alarms at multiple locations. The program's documentation shall describe the processes as to how the licensee would assess and respond to unauthorized access.

These requirements also apply at temporary job sites. Additionally, when transporting radioactive material quantities of concern to and from a temporary jobsite, detection and assessment capability shall be maintained when the transport vehicle is stopped at a hotel, restaurant, gas station, or other location.

In the event of any actual or attempted theft, sabotage, or diversion of radioactive material quantities of concern or the device, the licensee shall notify the local law enforcement agency (LLEA) immediately, followed soon thereafter by a call to the NRC Operations Center at (301) 816-5100, or, for Agreement State licensees, the appropriate Agreement State regulatory agency. Telephone calls to notify the NRC or State regulatory agencies should be as prompt as possible, but not at the expense of causing delay or interfering with LLEA response to the event.

Licensees shall have a prearranged plan with the LLEA that will respond to an actual or attempted theft of radioactive material quantities of concern or the device. One of the purposes of establishing liaison with the LLEA is to provide them with an understanding of the potential consequences associated with theft or sabotage of the radioactive material of concern so that the LLEA can appropriately determine the priority of its response. Licensees should inform the LLEA of the quantities of radioactive material that may be involved and the potential hazards associated with loss of control of the material. The licensee should also provide any facility information important to preplanning for an event response, establish licensee points of contact for recovery plans and radiation protection education, and work with the LLEA to develop a plan for a timely response. Licensees should determine, with the LLEA, the preferred method for contacting them to assure a timely response. The plan shall be consistent in scope and timing with realistic potential vulnerability of sources containing radioactive material quantities of concern (i.e., greater quantities require a faster response time and more response personnel. The pre-arranged plan shall be updated when changes to the facility design or operation affect the potential vulnerability of the sources.

A pre-arranged plan with the LLEA is not required at temporary job sites. However, licensees must still meet the requirements of IC 2.a. by immediately requesting assistance from the appropriate LLEA with jurisdiction for the area, of any actual or attempted theft, sabotage, or diversion of radioactive material quantities of concern or the device. When making a notification to the LLEA at a temporary job site, provide the LLEA with the quantities of radioactive material involved and the potential hazards associated with loss of control of the material.

As required by IC 2.c., it is necessary that the licensee have a dependable means to transmit information to the various components involved in the detection and assessment of an intrusion, including with the appropriate responder. Land line phones, auto dialers, cellular phones, pagers, radios, and other similar modes of communication may be used to fulfill this requirement. Using a radio or cellular phone as a backup to land line phones should be considered. When more than one person is used for detection and assessment, a means of communicating among the various monitoring personnel shall be provided.

Licensees shall establish written procedures for responding to events ranging from an inadvertent unauthorized access that would not require an LLEA response, to a malevolent intrusion that would require intervention by LLEA. These procedures should include provisions for immediate response, after-hours notification, handling of each type of emergency, events at temporary job sites, and the appropriate roles of the licensee's staff. The licensee staff should have a clear understanding of their responsibilities and limitations in an emergency, along with step-by-step instructions and clear guidelines for whom to contact. Note, that when developing enhanced control measures, the licensee should not compromise facility operational safety, occupational safety, fire safety, and emergency planning at the facility. Implementation of enhanced control measures should enhance safety.

Licensees should amend their training program for employees to include the licensee's procedures for implementing these requirements. Training should address the access control system employed and notification procedures in the event of an unauthorized access and potential malevolent activities. It should also include the process for reporting any suspicious activities to management.

Coordination of Radioactive Material Shipments

The objective of these requirements is to ensure timely detection of any loss or diversion of shipments containing radioactive material quantities of concern so that the licensee can initiate an appropriate investigation and response.

When shipping quantities of radioactive material greater than Table 1 values, per consignment, by a carrier other than by the licensee, the licensee shall seek reasonable assurance the carrier meets each of the requirements of IC 3.a. If the carrier has a tracking and security plan that the U.S. Department of Transportation requires for shipments of highway route quantities of radioactive material, the licensee shall verify and document that the carrier's tracking and security plan meets each of the requirements of IC 3.a, or obtain written confirmation that the carrier will implement these provisions.

As required by IC 3.b., licensees shall notify the NRC, in writing, 90 days before the anticipated date of shipment of radioactive material that exceeds 100 times the Table 1 quantities, per consignment. The NRC has Additional Security Measures (ASMs) for transportation of Radioactive Material in Quantities of Concern (RAM QC) which the Commission has determined are Safeguards Information - Modified Handling (SGI-M). SGI-M must be protected from unauthorized disclosure and no person may have access to SGI-M unless the person has an established need to know for the information. SGI-M related to the transportation of RAM QC must be protected in accordance with the Commission's November 5, 2004, order imposing SGI-M handling requirements on such information. That order can be found in the Federal Register at 69 Fed. Reg. 65470 (November 12, 2004). Because this group of licensees is not expected to be regularly shipping RAM QC, the NRC does not intend to release this SGI-M to licensees unless there is a demonstrated need to know. When a licensee notifies the NRC that it intends to ship such material, the NRC would then issue an additional Order for the transportation ASMs. Unless notified otherwise, in writing, by the NRC, licensees shall not ship the material before implementing the RAM QC transportation ASMs.

Once the licensee has implemented the ASMs, the licensee shall be exempt from the notification requirements of IC 3.b. for future shipments of radioactive material above Table 1 quantities, per consignment. However, the licensee is not exempt from other transportation reporting requirements. The licensee shall implement the additional controls for all future shipments of radioactive material above Table 1 quantities, per consignment.

If a manufacturer and distributor (M&D) licensee takes possession of the radioactive material at the shippers facility and ships the radioactive material under its M&D license, or implements the Transportation RAM QC ASMs for the shipping licensee, the licensee subject to this requirement shall be exempt from the requirements in IC 3.a. and IC 3.b.

When the licensee transports licensed radioactive material quantities of concern (e.g., to and from a temporary job site), the requirements of IC 1 and IC 2 shall be met.

Physical Barriers

Due to ease of movement, mobile and portable devices are particularly vulnerable to attempted theft or diversion; it may be possible for a mobile device to be removed before the licensee has an opportunity to respond to an intrusion. The objective of this requirement, therefore, is to delay an unauthorized entity long enough to provide additional time for the licensee and the LLEA to respond. This requirement requires licensees to have two independent physical controls that form tangible barriers to prevent unauthorized removal of mobile devices that are intended to be moved outside the facility (e.g., that are on trailers) and portable devices containing radioactive material quantities of concern that are not in use.

Examples of two independent physical controls at a licensed facility are:

- storage inside a locked storage shed within a secured outdoor area, such as a fenced parking area with a locked gate; or
- storage in a room with a locked door within a secured building for which access is controlled by lock and key or by a security guard; or
- storage inside a locked, non-portable cabinet inside a room with a locked door if the building is not secured.

Examples of two independent physical controls when securing the radioactive material quantities of concern in or on a transportation vehicle are:

- stored in a box physically attached to a vehicle, and the box is secured with two independent locks; two separate chains or steel cables that are locked and attached independently to the vehicle in such a manner that the box cannot be opened without the removal of the chains or cables; or
- stored in a box in a locked trunk, camper shell, van, or other similar enclosure and is physically secured to the vehicle by a locked chain or steel cable in such a manner that one would not be able to open the box and remove the portable or

mobile device without removal of the chain or cable.

Examples of two independent physical controls when at a temporary jobsite or at locations other than a licensed facility or licensee's vehicle, are:

- stored inside a locked building, in a locked non-portable structure (e.g., construction trailer, sea container, etc.), or in a locked garage, and is physically secured by a locked chain or steel cable to a non-portable structure in such a manner that an individual would not be able to remove the device without removing the chain or cable. A source must be inside a locked, non-portable cabinet or locked box that is secured to a non-portable structure.

- stored in a locked garage, and is within a locked vehicle or is physically secured by a locked chain or steel cable to the vehicle in such a manner that an individual would not be able to remove the device without removing the chain or cable.

For devices in or on a vehicle or trailer, licensees shall also utilize a method to disable the vehicle or trailer when not under direct control and constant surveillance by the licensee. Examples of acceptable methods include: trailer hitch locks, wheel locks ("boots"), or methods to disable the vehicle's engine.

For mobile devices that are used inside a facility, additional delay may be accomplished by a variety of physical controls, including:

- speed bumps on floor too large for device to traverse ;
- elevated doorway thresholds;
- protective storage enclosures;
- channels in floor large enough to catch the device wheels;
- wheel locks (made of hardened material) that require key or special tool to release; or
- a hardened chain and lock that cannot be easily cut.

The additional physical controls should not compromise safety. If improperly implemented, some of the suggested items may compromise occupational safety.

Information Protection

The information generated by licensees which must be protected is information about its physical protection (security and controls) for radioactive material of concern, and includes but is not limited to: information describing how the radioactive material is secured from unauthorized removal or access when it is in storage, information describing how the licensee controls and maintains constant surveillance of the radioactive material when not in storage, information describing specific policies and procedures for actions taken by the licensee in response to the increased controls, and the details of the enhancements implemented for the

radioactive material covered under this requirement. Such information is referred to as "sensitive information."

The following discussion provides guidance licensees should follow to ensure compliance with the information protection requirements fo IC 6:

(1) the licensee's policies and procedures must include general performance requirement that each person who produces, receives, or acquires the licensee's sensitive information to ensure that such information is protected against unauthorized disclosure;

Dissemination of licensee's sensitive information is limited to individuals who have an established need-to-know and who are trustworthy and reliable. Other than those individuals authorized by the licensee, members of certain occupational groups may be deemed trustworthy and reliable by virtue of their employment status. These occupational groups are:

1. An employee, agent, or contractor of the Commission, or the United States Government;
2. A member of a duly authorized committee of the Congress;
3. The Governor of a State or his designated representative;
4. A representative of the International Atomic Energy Agency (IAEA) engaged in activities associated with the U.S./IAEA Safeguards Agreement who has been certified by the NRC;
5. A member of a state or local law enforcement authority that is responsible for responding to requests for assistance during security emergencies; or
6. A person to whom disclosure is ordered pursuant to Section 2.709(f) of Part 2 of Part 10 of the Code of Federal Regulations.
7. State Radiation Control Program Directors (and State Homeland Security Directors) or their designees.

If there is any indication that the recipient would be unwilling or unable to provide proper protection for the licensee's sensitive information they should not be authorized to receive it.

(2) the licensee's policies and procedures must address how to protect sensitive information while in use, storage, and transit;

The licensee should store the information in a locked cabinet, desk, office, etc. Information stored in non-removable electronic form should be password protected. Licensees need to address how employees need to protect the sensitive information while in their possession both at and away from the office. Access to the keys, combinations, passwords or other means used to secure the information needs to be limited to those persons authorized.

(3) the licensee's policies and procedures must address the preparation, identification or marking, and transmission of documents or correspondence containing the licensee's sensitive information;

The licensee generated sensitive information should be marked in such a manner to assure easy identification and to ensure proper handling. The front and back of folders containing sensitive information should be marked for easy identification and to ensure proper handling.

Documents that do not in themselves contain sensitive information but are used to transmit one or more documents containing this information should be marked to indicate the fact that sensitive information is contained in the documents transmitted. Transmittals to the NRC should be marked: "**Withhold from Public Disclosure in Accordance with 10 CFR 2.390.**" For Agreement State licensees, transmittals should be marked in accordance with equivalent Agreement State requirements. These markings should be placed at the top and bottom of only the first page of the transmitted document.

(4) the licensee's policies and procedures must address how access to the licensee's sensitive information is controlled;

Dissemination of sensitive information by licensees must be limited to individuals that have a "need-to-know" a licensee's security information to perform their job duties, and are determined trustworthy and reliable using criteria consistent with those requirements in IC 1. Access by licensee employees, agents or contractors must include both an appropriate need-to-know as determined by the licensee, as well as an appropriate determination concerning the trustworthiness and reliability of individuals having access to the information. Employees of an organization affiliated with the licensee's company, e.g., a parent company, may be considered as employees of the licensee for access purposes. Licensee's should assure that individuals not authorized to receive such information do not overhear conversations relating to the substantive portions of the sensitive information.

(5) the licensee's policies and procedures must include acceptable methods for destruction of documents containing sensitive information;

Documents containing sensitive information should be destroyed by a method that will prevent reconstruction of the information. Documents may be destroyed by tearing them into small pieces or by burning, pulping, pulverizing, shredding, or chemical decomposition. (Note: sensitive information should not be sent to recycling without being destroyed first)

(6) the licensee's policies and procedures must include use of automatic data processing systems containing sensitive information;

Sensitive information may be processed or produced on an Automated Information System (AIS) provided that the user is appropriately briefed on the proper procedures

while using the computer system. Individuals should protect the information during use by maintaining control and by ensuring only individuals with the appropriate "need-to-know" have access to the information.

(7) the licensee's policies and procedures address removing documents from the licensee's sensitive information category when they become obsolete or no longer sensitive.

Periodic review of documents containing sensitive information to determine whether these documents should remain in this category is not required. However, this review is necessary only when specific circumstances require such action.

Definitions

Access Control - A means to allow only those individuals approved by the licensee, unescorted access to radioactive material.

Assessment - Licensee's capability to ascertain cause of alarm condition.

Approved Individual - Those individuals who the licensee has determined are trustworthy and reliable based on an appropriate verification.

Consignment - A package or group of packages of radioactive material that a licensee offers for transport in the same shipment.

Delay - To impede or hinder the progress of an intruder.

Dependable means to Transmit Information - Intrusion detection system and components which are used to detect, inform assessor(s), and summon responder(s), such that the system and components have continuous or alternate communication capability, even in the event of the loss of primary power or the loss of primary communication means.

Detect - To discover all unauthorized access to the radioactive material quantities of concern or device.

Radioactive material quantities of concern - Licensed radioactive material that individually or in aggregation is greater than the quantities in Table 1. The unity rule is used to determine if the activity of aggregated sources of different radionuclides is greater than the Table1 quantities (see discussion following Table 1).

Immediately detect, assess, and respond - Detect, assess, and respond without delay.

LLEA - Any local law enforcement agency at the State level and below to include local jurisdictions.

Mobile device - A device containing licensed radioactive material that is mounted on a permanent base with wheels and/or casters for moving while completely assembled. Portable equipment means a device containing licensed radioactive material that is designed to be hand-carried, and stationary equipment means a device containing licensed radioactive material which is installed in a fixed location.

Monitor - Capability to observe and detect unauthorized access.

Need-to-know - means a determination, by a person having responsibility for protecting the licensee's sensitive information, that a proposed recipient's access to the licensee's sensitive information is necessary in the performance of official, contractual, or licensee duties of employment.

Plan with LLEA - A plan which is consistent in scope and timing with realistic potential vulnerability such that the LLEA acknowledges they can provide a timely response to thwart unauthorized actions.

Reliable and Trustworthy - An individual who is considered consistently dependable in judgement, character, performance, and does not constitute an unreasonable risk ti the public health and safety.

Timely Response - Arrival of LLEA or armed responder to thwart unauthorized access and unauthorized actions associated with radioactive material quantities of concern or device.