Results from Increased Control inspections performed during the first year has demonstrated a

DISCONNECT

This pamphlet provides guidance to help Texas industrial radiography licensees understand and comply with the Increased Control requirements most commonly cited as violations.

The failure of industrial radiography licensees to adequately implement the increased security requirements for radioactive material quantities of concern has resulted in enforcement actions that include:

1. Assessment of monetary penalties up to $24,000;

2. Valuable time lost attending one or more enforcement conferences in Austin; and,

3. A recommendation to revoke a radioactive material license.

Increased Control (IC) security inspections are performed annually by the agency. During the inspectors' next visit, the effectiveness of your commitment to correct any previous violations will be verified. If not corrected, a repeat violation will be issued, and enforcement action may result. This information is provided to help avoid repeat violations.

Increased Control Requirement 1

The trustworthy and reliable (T&R) determination is designed to identify past actions to help verify one's character and reputation. This should provide reasonable assurance of an individual's future reliability. It is the licensee's decision as to what criteria is used for the basis of the T&R determination.

3 Steps to Determine an Individual is T&R:

1. Document that you have verified the individual's education, work history and references.

2. Document the reason (basis) that each individual will be granted unescorted access to your radioactive material (RAM).

3. Create a list of the people approved to have unescorted access to your RAM.

T&R documentation must include each individual's name, basis used to develop the determination, (including the criteria and supporting documentation), the date you determined them to be T&R, and the name and signature of the person responsible for making the determination.

Reasons a violation is cited:

- The 3 steps for determining T&R of each individual was not documented.

- No T&R list.

- Names of individuals are included on the T&R list, even though all required T&R steps had not been completed.

- Unapproved individuals are granted unescorted access to RAM.

Increased Control Requirement 2

Detect, Assess & Respond:

The objectives are to reduce the risk of theft of RAM, to prevent its unauthorized use and to improve the opportunity for recovery, if stolen. You must have and document a program to:

- Immediately detect unauthorized access to RAM;
- Assess whether the unauthorized access was an actual or attempted theft; and,
- Initiate an appropriate response.

Controlling Access to RAM:

You must restrict unescorted access to only individuals that have been determined to be T&R, and must have access to do their job.

Examples of achieving controlled access to RAM:

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

These requirements also apply at temporary job sites. When transporting RAM, including the device, to and from a temporary jobsite, access control must be maintained at all times, including times when the transport vehicle is stopped at a hotel, restaurant, gas station, or other location.

Reasons a violation is cited:

- No written procedure for controlling access.
- Consultant-generated "generic" procedure is not modified to address your program to detect access and respond.
- RAM is not secured or under constant surveillance at all times (i.e. 24/7).

Increased Control Requirement 2

Reason a violation is cited (cont.):

- Security system fails to alert you as designed. A security system should be tested routinely to make sure it is not disarmed, functions properly, and the proper sensitivity is set to eliminate false alarms.

Prearranged Plan with Local Law Enforcement Agency (LLEA):

Coordination with LLEA is essential in developing an effective and efficient program to respond to events. Documentation must include your efforts to coordinate with LLEA, and any cases where the LLEA chooses not to participate in a formal response plan. The pre-arranged plan should include the important aspects of your physical protection program and other factors that would aid the LLEA to appropriately prioritize and respond to an alarm. Examples of information which could be discussed with LLEA and incorporated into a pre-arranged plan include, but are not limited to:

- Type and quantity of RAM that may be involved;
- Potential hazards associated with loss of control of RAM;
- Specific facility information (floor plans, entrances, points of egress);
- Potential for removal of sources from devices or removal of the device as a whole;
- A realistic potential vulnerability of the RAM;
- Site-specific physical protection you use to delay an adversary from gaining access to the RAM before LLEA can arrive;
- Established protocol for contacting LLEA in response to an event;
- Points of contact for RAM recovery plans;
- Radiation protection education for LLEA.

Reason a violation is cited:

- No written document of your prearranged plan.

Increased Control Requirement 6

Protection of Sensitive Information:

Procedures must be developed that describe how to handle and protect sensitive information and must include:

1. A general performance requirement that states how each person who produces, receives or acquires your sensitive information will protect the information from unauthorized disclosure;

2. How sensitive information will be protected at, or away from, the storage site (how access to the location of sensitive information is restricted);

3. How sensitive information will be marked to assure easy identification and proper handling;

4. How your sensitive information will be controlled, and access limited to only those individuals that have a need-to-know;
   - individuals given access to sensitive information must have a need-to-know your security information to do their job duties; and,
   - individuals with a need-to-know must be determined to be T&R using the 3 steps previously described;

5. How documents containing sensitive information will be destroyed and how to prevent re-creation or recovery of the information;

6. How information generated by, or stored in, any computer system will be secured against unauthorized access; and,

7. How a document containing sensitive information will be reviewed and removed from this category when it is no longer sensitive.

Increased Control Requirement 6

What is Sensitive Information?

Any information about the physical protection of your RAM is considered sensitive information and it must be protected.

Examples of sensitive information include, but are not limited to:

- The location of your RAM;
- How RAM is secured from unauthorized access or removal when in storage;
- How you will control access and provide continuous monitoring when RAM is not in storage (at a temporary job site, etc.); and,
- The specific details of enhancements and procedures implemented in response to the IC requirements.

Reasons a violation is cited:

- No written procedure for protection of sensitive information.
- Consultant-generated “generic” procedure is not modified to specifically address how the licensee handles and protects its sensitive information.
- Sensitive information was provided to someone who did not have a need-to-know and/or was not determined to be T&R.

Nuclear Regulatory Commission guidance documents are located at: http://www.nrc.gov/reading-rm/doc-collections/enforcement/security/index.html, under the heading “Holders of Material Licenses Authorized to Possess Radioactive Material Quantities of Concern.”

TEXAS Department of State Health Services

Produced by the Texas Department of State Health Services 2007