



Radiological Safety Division

S.A. Hussain
Head, RSD

Fax No. (022) 25990650
Email: sahussain@aerb.gov.in

Ref. No. AERB/RSD/IR-Security/2011/ 12885

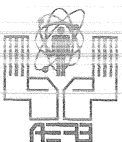
October 28, 2011

Sub: Physical security for Industrial Gamma Radiography Exposure Devices (IGREDs)

We hereby draw your attention to the recent incidents involving theft of Industrial Gamma Radiography Exposure Devices (IGREDs)/Radiography Cameras containing ¹⁹²Ir sources. One of the IGREDs was stolen during use while the other from the storage room. You would realize that such incidents may lead to serious radiological consequences involving workers and members of public, if stolen/lost IGREDs are handled unsafely by unauthorized personnel or tampered with inadvertently.


In the light of these serious incidents, it is advised that your institution should ensure the physical security of radiation sources in your possession during their use, storage as well as during transport. It should be noted that as per Rule 20 (2) of Atomic Energy (Radiation Protection) Rules, 2004, it is the responsibility of employer to ensure physical security of the sources at all times as the custodian of radiation sources in his possession. Any untoward incident involving radiation sources would be viewed seriously by this Division and may lead to enforcement of appropriate regulatory action against such institutions under Atomic Energy (Radiation Protection) Rules, 2004.

With regard to the guidelines for security of radioactive sources, the Atomic Energy Regulatory Board has published the Safety Guide on "Security of Radioactive Sources in Radiation Facilities" {No. AERB/RF-RS/SG-1} and "Security of Radioactive Material During



Transport" {No. AERB/NRF-TS/SG-10}. You may refer these guides which have been made available on our website www.aerb.gov.in . For ready reference, extract of the guidelines given in these guides pertaining to industrial gamma radiography devices is enclosed herewith – as Annexure-I & Annexure-II respectively.

It shall be ensured by every user of radioactive sources that the applicable security plan is in place and shall be implemented immediately. Should you require any further clarification in this regard, please contact the undersigned or Dr. A. U. Sonawane (Tel. No. 022-25990657, email: ausonawane@aerb.gov.in).


28.10.11
(S. A. Hussain)

Distribution: All institutions possessing IGREDs / Supplier of IGREDs / Supplier of

Radiography Sources

(Extract from AERB Safety Guide No. AERB/RF-RS/SG-1)

Annexure-I-a

**GUIDELINES TO PREPARE SECURITY PLAN FOR INDUSTRIAL GAMMA
RADIOGRAPHY**

(SOURCE CATEGORY 2 AND SECURITY LEVEL-B)

As regards the four security functions, the security plan should indicate the specific measure(s), which would be implemented to meet the security objectives. Given below are the security objectives against each of which, some security measures have been suggested. Specific details of these measures should be furnished in the security plan. It may be noted that these guidelines by no means are comprehensive.

Detection

1. Security objective: Provide immediate detection of unauthorised access to the secured area / source location.
Security measures: Electronic intrusion detection system and/or continuous surveillance by operating personnel.
2. Security objective: Provide immediate detection of any attempted unauthorised removal of the source.
Security measures: Tamper detection equipment and/or continuous surveillance by operating personnel.
3. Security objective: Provide immediate assessment of detection.
Security measures: Remote monitoring of CCTV or assessment by operator/ response personnel. Movement of the radiography device/ source outside the controlled area should be constantly monitored by trained persons.
4. Security objective: Provide immediate communication to response personnel.
Security measures: Rapid, dependable means of communication such as phones, cell phones, pagers, radio links.
5. Security objective: Provide a means to detect loss through verification.
Security measures: Weekly checking through physical checks, tamper indicating devices, etc.

Delay

1. Security objective: Provide delay after detection sufficient for response personnel to interrupt the unauthorised removal.

Security measures: System of two layers of barriers (e.g. walls, cages). The gate pass for taking a source out of the radiation facility should require multiple authorisations from different agencies.

Response

1. Security objective: Provide immediate initiation of response.

Security measures: Capability for timely response with size, equipment and training.

Security Management

1. Security objective: Provide access controls to source location that permits access to authorised persons only.

Security measures: One identification measure, e.g., lock controlled by swipe card reader or personal identification number, or key and key control.

2. Security objective: Ensure trustworthiness for individuals involved in the management of sources.

Security measures: Background checks for all personnel authorised for unescorted access to the source location and for access to sensitive information.

3. Security objective: Identify and protect sensitive information.

Security measures: Procedures to identify sensitive information and protect it from unauthorised disclosure.

4. Security objective: Provide a security plan.

Security measures: A security plan which conforms to regulatory requirements and provides for response to increased threat levels.

5. Security objective: Ensure a capability to manage security events covered by security contingency plans.

Security measures: Procedures for responding to security-related scenarios.

6. Security objective: Establish security event reporting system.

Security measures: Procedures for timely reporting of security events.

Annexure-I-b
KEY ISSUES TO BE CONSIDERED IN A SECURITY PLAN

A security plan should include all relevant information required to evaluate and to understand the security concept being used for the source. The following topics would typically need to be included.

- (a) A description of the sources and their use and security level(s).
- (b) A description of the environment, building and/or facility where the source is used or stored, and if appropriate a diagram of the facility layout and security system.
- (c) The location of the building or facility relative to areas accessible to the public.
- (d) The perceived security threats and the basis of such perception.
- (e) The objectives of the security plan for the specific application, including:
 - (i) the specific concern to be addressed: theft, destruction, or malevolent use;
 - (ii) the kind of control needed to prevent undesired consequences including the auxiliary equipment that might be needed; and
 - (iii) the equipment or premises that will be secured.
- (f) The technical measures to be used, including:
 - (i) the measures to secure, provide surveillance, provide access control, detect, delay, respond and communicate; and
 - (ii) the design features to evaluate the quality of the measures against the assumed threat.
- (g) The administrative measures to be used, including:
 - (i) the security roles and responsibilities of management, staff and others;
 - (ii) routine and non-routine operations, including accounting for the sources(s);
 - (iii) maintenance and testing of equipment;
 - (iv) determination of the trustworthiness of personnel;
 - (v) the application of information security;
 - (vi) methods for access authorization;
 - (vii) security related aspects of the emergency plans, including event reporting;
 - (viii) training; and
 - (ix) key control procedures
- (h) References to existing regulations or standards
- (i) Periodic updating of the security plan to ensure its continued effectiveness
- (j) Procedure for reporting security related events
- (k) Periodic evaluation of security systems for their functional performance
- (l) Methods to ensure continued functionality of the security systems.

{Extract from AERB Safety Guide No. AERB/NRF-TS/SG-10}

Annexure-II

For Gamma Radiography Exposure Devices (IGRED) the applicable security level is Security Level 3. The measures detailed in for Level-3 should be adopted in addition to the Prudent Management Practices i.e. Security Level 1 and Basic Security Measures i.e. Security Level 2.

III.1 Level 1 - Prudent Management Practices

The security measures in this level should include by not limited to the following.

The consignor to have formal systems in place for:

- i. Accounting the radioactive source.
- ii. Proper selection of a carrier.
- iii. Prompt notification to the consignee regarding the dispatch of the consignment.
- iv. Keeping track of the consignment during its movement in the public domain and formal confirmation of the receipt of the consignment by the consignee.

III.2 Level 2 - Basic Security Measures

The security measures in this level should include by not limited to the following.

- i. General Security Provisions:
 - Only properly authorised operators should be involved in the transport of radioactive materials. Normally, the existence of good business relationship between a carrier and consignee/consignor can be considered as sufficient;
 - The operator should have a systematic procedure, which would continually give the status on the position of the package and alert the operator when packages are not delivered to the intended recipient at the expected time. As soon as it is determined that a package has been lost or stolen, actions should be immediately initiated to locate and recover the package;
 - When radioactive materials are to be temporarily stored in transit sites, appropriate security measures as would have been applied for the material during transport or use and storage shall be applied.
- ii. Provision of security locks.
- iii. Training of personnel on security awareness.
- iv. Identity verification of personnel and conveyances.
- v. Security related information exchange among the Consignors, Consignees and Carriers.
- vi. Verification of trustworthiness of personnel.

The antecedents and trustworthiness of persons engaged in transport of radioactive material should be got verified from the appropriate authorities. The extent of verification should be commensurate with the responsibility of the person involved in transportation.

III.3 Level 3 - Enhanced Security Measures

The security measures in this level should include by not limited to the following.

i. Availability of Formal Security Plans

The operators and all persons engaged in the transport of radioactive material that require enhanced security level should develop, adopt and implement a security plan. As a minimum requirement the security plan should include the following:

- Specific allocation of responsibilities for security to qualified and competent persons with appropriate authority to carry out their responsibilities;
- Review of current operation to assess vulnerability, temporary transit storage, handling, distribution etc.;
- Clear statements of measures regarding training, policies (response to higher threat conditions, new employee verification), operating practices (e.g. choice of routes, use of guards and their placement and positioning, controlling access to radioactive material packages in storage) equipment and resources that are required to reduce security risk;
- Effective procedures and equipment for prompt reporting and dealing with security threats, breaches of security or security incidents;
- Procedures for evaluating and testing security plans;
- Procedures for review and update of the plans;
- Measures to ensure that sensitive transport information is sent only to concerned agencies to maintain security. However, these measures shall not preclude provisions of transport documents and consignor's declaration as required by applicable transport regulations;
- Measures to monitor the shipment; and
- Arrangements to define the transfer of responsibility for the security of the package wherever necessary.

ii. Wherever possible, appropriate tracking devices (e.g. GPS) should be used to monitor the movement/shipments of conveyances containing radioactive material.

iii. Provision of Communication Links:

The carrier should provide a communication system during transport to enable the personnel to communicate with a designated contact point as specified in the security plan.