GUIDE NO. AERB/RF-RS/SG-1

GUIDE NO. AERB/RF-RS/SG-1

GOVERNMENT OF INDIA

AERB SAFETY GUIDE

SECURITY OF RADIOACTIVE SOURCES IN RADIATION FACILITIES

ATOMIC ENERGY REGULATORY BOARD

AERB SAFETY GUIDE NO. AERB/RF-RS/SG-1

SECURITY OF RADIOACTIVE SOURCES IN RADIATION FACILITIES

Atomic Energy Regulatory Board
Mumbai-400 094
India

March 2011

Price

Order for this guide should be addressed to:

The Administrative Officer
Atomic Energy Regulatory Board
Niyamak Bhavan
Anushaktinagar
Mumbai-400 094
India

FOREWORD

Activities concerning establishment and utilisation of nuclear facilities and use of radioactive sources are to be carried out in India in accordance with the provisions of the Atomic Energy Act, 1962. In pursuance of ensuring safety of members of the public and occupational workers as well as protection of environment, the atomic energy regulatory board (AERB) has been entrusted with the responsibility of laying down safety standards and enforcing rules for such activities. The Board has, therefore, undertaken a programme of developing safety standards, safety codes, related guides and manuals. While some of these documents cover aspects such as siting, design, construction, operation, quality assurance and decommissioning of nuclear and radiation facilities, other documents cover regulatory aspects of these facilities.

Safety codes and safety standards are formulated on the basis of internationally accepted safety criteria for design, construction and operation of specific equipment, systems, structures and components of nuclear and radiation facilities. Safety codes establish the objectives and set requirements that shall be fulfilled to provide adequate assurance for safety. Safety guides and guidelines elaborate various requirements and furnish approaches for their implementation. Safety manuals deal with specific topics and contain detailed scientific and technical information on the subject. These documents are prepared by experts in the relevant fields and are extensively reviewed by advisory committees of the Board before they are published. The documents are revised when necessary, in the light of experience and feedback from users as well as new developments in the field.

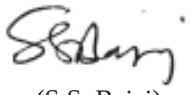
In India, radiation sources are being widely used for societal benefits in industry, medical practices, research, training and agriculture. It has been reported from all over the world that unsecured radioactive sources caused serious radiological accidents involving radiation injuries and fatalities. Particular concern was expressed regarding radioactive sources that have become orphaned (not under regulatory control) or vulnerable (under weak regulatory control and about to be orphaned). There is a concern about safety and security of radioactive sources and hence the need of stringent regulatory control over the handling of the sources and their security. In view of this, this guide is prepared which gives provisions necessary to safeguard radiation installations against theft of radioactive sources and other malevolent acts that may result in radiological consequences. It is, therefore, required that the radiation sources are used safely and managed securely by only authorised personnel. This guide is intended to be used by users of radiation sources in developing the necessary security plan for sources.

Consistent with the accepted practice, ‘shall’ and ‘should’ are used in the guide to distinguish between a firm requirement and desirable option respectively. Appendices and bibliography are included to provide further information on the subject that might be helpful to the user. Approaches for implementation, different to those set out in the

guide may be acceptable, if they provide comparable assurance against undue risk to the health and safety of the occupational workers and the general public, and protection of the environment.

Specialists in the field drawn from the Atomic Energy Regulatory Board, the Bhabha Atomic Research Centre, the Board of Radiation & Isotope Technology, the Department of Atomic Energy and other consultants have prepared this guide. It has been reviewed by experts and relevant AERB Advisory Committee on Codes and Guides.

AERB wishes to thank all individuals and organisations who have prepared and reviewed the draft and helped to finalise it. The list of persons, who have participated in this task, along with their affiliations, is included for information.



(S.S. Bajaj)
Chairman, AERB

DEFINITIONS

Atomic Energy Regulatory Board (AERB)

A national authority designated by the Government of India having the legal authority for issuing regulatory consent for various activities related to the nuclear and radiation facility and to perform safety and regulatory functions, including their enforcement for the protection of site personnel, the public and the environment against undue radiation hazards.

Design Basis Threat (DBT)

The attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorised removal of nuclear material or sabotage, against which a physical protection system is designed and evaluated.

Radiation Facility

Any installation/equipment or a practice involving use of radiation-generating units or use of radioisotopes in the field of research, industry, medicine and agriculture.

Radiation Surveillance

Measures that may be specified by the competent authority to provide adequate protection either generally or in any individual case.

Radioactive Material/Radioactive Substance

Any substance or material, which spontaneously emits radiation in excess of the levels prescribed by notification by the Central Government.

Sealed Source

Radioactive source material that is (a) permanently sealed in a capsule, or (b) closely bounded and in a solid form. The capsule or material of a sealed source shall be strong enough to maintain leak tightness under the conditions of use and wear for which the source was designed, as also under foreseeable mishaps.

Source

Anything that may cause radiation exposure, either by emitting ionising radiation or releasing radioactive substances or materials.

CONTENTS

1. INTRODUCTION

1.1 General

Radioactive sources are widely used in various applications in medicine, industry and research. These sources are supplied by authorised manufacturers to authorised users and the Atomic Energy Regulatory Board (AERB) is the authority empowered to issue such authorisations.

Unsecured sources can cause serious injuries and could even result in fatalities. Further they could also result in damage to the environment and lead to significant economic losses. In India, this issue of security of sources was addressed as early as in 1980, when a notification titled 'The Industrial Radiography (Radiation Surveillance) Procedures [1]' was issued under the Radiation Protection Rules, 1971 [2], which identified the licencee as being responsible for the security[1] of the source. As per the Atomic Energy (Radiation Protection) Rules, 2004 [3] issued under the Atomic Energy Act, 1962, a licence needs to be obtained from the Competent Authority for handling such sources. The Atomic Energy (Radiation Protection) Rules, 2004 also emphasise the importance of the security of radioactive material, in addition to radiological safety.[2]

International Atomic Energy Agency (IAEA) in 1996, published the International Basic Safety Standards for Protection against Ionising Radiation and for the Safety of Radiation Sources (BSS) [4], which specifically requires that sources shall be kept secure so as to prevent theft or damage. The IAEA code of conduct on the safety and security of radioactive sources [5] addresses the matter of security of sources extensively and recommends that appropriate measures be taken to ensure that the radioactive sources are safely managed and securely protected during and till their useful lives, and until their safe disposal. It also recommends that safety culture[3] and security culture[4] should be promoted.

Any breach in security during the handling of radioactive material, could have safety consequences resulting in radiation exposure to workers and/or

---

1 Security means measures to prevent unauthorised access or damage to, and loss, theft or unauthorised transfer of, radioactive sources.

2 Radiological safety means measures intended to minimise the likelihood of accidents with radioactive sources and, should such an accident occur, to mitigate its consequences.

3 Safety culture means the assembly of characteristics and attitudes in organisations and individuals, which establishes that, as an overriding priority, protection and safety issues receive the attention warranted by their significance.

4 Security culture means characteristics and attitudes in organisations and of individuals, which establish that security issues receive the attention warranted by their significance.

the public, in excess of the regulatory dose limits. Accordingly, the AERB has taken up the task of developing the technical basis to establish security levels for ensuring the safety of radioactive materials during all stages of their handling. Recognizing the need to ensure appropriate use of the sources for beneficial purposes it is intended that the level of security should be commensurate with the potential hazard posed by the sources. Towards this, measures have to be applied to prevent unauthorised access, loss, theft and unauthorised transfer of radioactive sources at all stages of their life cycle. Safety and security aspects of sources are intimately linked and many of the measures designed to address safety would also address security. However, in the current context, consideration needs to be given to the possibility that these may not be sufficient to address the threat of deliberate attempts to acquire control of a radioactive source for malevolent purposes. Based on the potential hazard and vulnerability of a source or device, as well as the potential consequences of any malevolent action, a graded concept of security measures is outlined in this guide. Implementation of these measures is expected to significantly lower the risk associated with such sources.

1.2 Objective

The security of radioactive sources includes measures required to protect the sources from unintentional access by inappropriately qualified personnel or attempts of theft for financial gain. The objective of this guide is to recommend to the employer and the licencee security measures which are aimed at prevention and countering of deliberate and malevolent acts that could result in significant radiological consequences. The recommended measures include a combination of deterrence, early detection and delay of attempts at unauthorised acquisition, mitigation of consequences and response to a loss of authorised control including recovery.

1.3 Scope

The guidance provided in this document address the radiological concerns / hazards associated with the unauthorised removal, sabotage and other intentional malicious acts during the handling of radioactive material which are used in medical, industrial and research applications. This document covers the processes to determine the level of security required for preventing malevolent use of sources throughout their lifecycle, and the assignment of security measures to sources based on graded performance requirements to deter, detect, and, if necessary respond to theft of radioactive material. In doing so, it is recognised that such measures will also minimise inadvertent or negligent losses of sources.

While security considerations for all radioactive sources are outlined in this document, the main focus is on radioactive sources that could be dangerous if they are not under control (primarily Categories 1 to 3 in Ref. [6]). The

security concerns addressed in this guide relate primarily to sealed sources. However, consistent with the code of conduct, the scope of this document includes unsealed sources also. This guidance applies to all medical, industrial and research institutions, nuclear facilities and radioactive waste disposal facilities. This guide is not applicable to nuclear material.[5]

This guidance has been drawn up for the following radioactive sources used by the above radiation and nuclear facilities:

(i) Reference sources

(ii) Consumer products (e.g. smoke detectors, luminous painted dials, tritium light sources)

(iii) Radiopharmaceuticals

(iv) Nucleonic gauge sources

(v) Calibration sources

(vi) Sources used in well logging

(vii) Industrial radiography sources

(viii) LDR Brachytherapy sources

(ix) HDR Brachytherapy sources

(x) Teletherapy sources

(xi) Gamma irradiator sources

(xii) Decayed sealed sources for disposal

The guidance specified in this report are applicable to the complete life cycle of sources covering manufacture, supply, receipt, storage, use, transfer, import, export, transport, operation, maintenance or disposal of radioactive sources. Since the security of radioactive sources in the public domain merit separate consideration, the guidance for the same are addressed in another AERB publication [7].

This document does not discuss radiation safety requirements for specific applications. These practice specific guidance outlined in other AERB publications should also be followed in addition to the guidance given in this document.

5 Nuclear material means plutonium except that with isotopic concentration exceeding 80% in ^{238}Pu; ^{233}U; uranium enriched in isotope 235 or, uranium containing the mixture of isotopes as occurring in nature other than in the form of ore or ore-residue; any material containing one or more of the foregoing.

2. SECURITY PRINCIPLES

2.1 Basic Principles of Security

In attempting to address the threats from malevolent acts involving radioactive sources, it is clear that sources of certain magnitudes and types are more vulnerable to such acts than others. Therefore, the approach to security needs to be graded accordingly. Following are components which would influence the strategy to be adopted while drawing up a specific security plan:

(a) Management[6] of sources only within an authorised, regulated, legal framework.

(b) Appropriate design and manufacture of sources and design features incorporated in the equipment housing the sources, to minimise the feasibility of malicious actions and maximise security.

(c) Prevention of acquisition of radioactive sources by those with malevolent intent. This includes measures to:

  (i) deter unauthorized access to the source or source location, in order to deter theft;

  (ii) detect any such attempts at unauthorised access;

  (iii) delay unauthorised access or theft;

  (iv) provide rapid response to attempts at unauthorised access or theft; and

  (v) ensure the reliability of personnel involved in managing sources.

(d) Detection of actual theft or loss in order to appropriately respond and allow recovery efforts to start as soon as possible. This includes:

  (i) the provision of radiation, or other alarms; and

  (ii) accounting[7] and inventory[8].

(e) Efforts to recover any stolen or lost sources and bring them into secure regulatory control.

---

6 Management means all activities, administrative and operational, that are involved in the manufacture, supply, receipt, storage, use, transfer, import, export, transport, maintenance or disposal of radioactive sources.

7 Accounting means physically checking that all sources are present in their expected location. This may be satisfied by an appropriate radiation survey.

8 Inventory means a campaign to physically check all sources possessed, by specifically and uniquely identifying each individual source using appropriate means such as serial numbers.

(f) Prevention of unauthorised use of sources.

(g) Minimisation of the consequences of any malevolent use of a source.

2.2 Security Culture

It is necessary that the radiation facility develops and maintains a security culture, which can be achieved by various means such as:

(i) identifying the personnel and their roles in ensuring the security of radioactive sources in the facility;

(ii) documenting a security plan which will also assign security responsibilities, and informing all the concerned employees and contractors of their specific roles;

(iii) providing security instructions and ongoing security awareness briefings to staff and contractor and training and evaluation of the lessons learned;

(iv) ensuring threat awareness and training security managers, response personnel and all personnel with secondary responsibilities for security; and

(v) conducting regular performance testing and preventive maintenance.

The security culture should be inculcated amongst all employees. This should be done by means of training and awareness programmes, security drills, etc. It is not only the persons who are occupationally exposed to radiation in the facility but also the general employees working in the facility should be included in such programmes. The employer, the licencee, the radiological safety officer (RSO) and the general security personnel have important roles to play in developing the security culture amongst all employees in the facility.

2.3 Security Functions

The security functions cover the entire gamut of activities required to ensure that radioactive sources are always under regulatory control. These functions range from simple safe management and protection of the sources to the establishment of systems that would prevent unauthorised access to the sources. The security functions deter and delay unauthorised access to sources, detect should such access occur and ensure that measures to mitigate the radiological consequences and recover the sources are implemented without delay. The basic security functions are deterrence, detection, delay, response and security management.

2.3.1 *Measures of Deterrence*

The measures of deterrence are aimed at convincing that act of getting unauthorised access to a source would be too difficult, that the success of the

act would be uncertain and that the consequences would not justify the risk of undertaking the act. Communicating the existence of such measures would to a large extent serve the purpose of such deterrence. In this regard, implementing specific measures for detection, delay, response and security management would themselves function as a deterrent.

2.3.2 *Measures of Detection*

The measures of detection are aimed at discovering an actual or an attempted intrusion, which could have the objective of theft or sabotage involving a radioactive source. Means of detection include visual observation, electronic surveillance (which include video surveillance like CCTVs, electric sensors, IR sensors, etc), periodic source accounting, seals and other tamper-indicating devices.

2.3.3 *Measures of Delay*

The measures of delay are aimed at impeding an adversary's attempt to gain unauthorized access or removal or sabotage of a radioactive source. This is generally achieved through barriers or other physical means. The effectiveness of delay is measured by the time required by the adversary to gain unauthorised access to the source and commit the intended malicious act.

2.3.4 *Measures of Response*

The measures of response are aimed at preventing a malicious act and if it occurs, mitigating the severity of the consequences of such an act. These measures have to be implemented by security personnel or the law enforcing personnel. The actions include interrupting and subduing an adversary while the malicious act is being committed or preventing the adversary from using a stolen radioactive source for committing a malicious act or mitigating the severity of the consequences of such an act.

2.3.5 *Measures of Security Management*

The measures of security management are aimed at developing procedures, policies, records and plans for the security of radioactive sources, proper handling of sensitive information and protecting it against unauthorised disclosure.

2.4 Assessment of Threat and Vulnerability

It is recommended that the best method to design security measures for specific sources is the use of a 'design basis threat (DBT) assessment' methodology. The DBT will vary quite widely from one location to another within the country, one type of facility and another and from source to source. The associated security measures should be commensurate with the threat and

the level of risk acceptance. The assessment of threat could range from being a generic one to a very detailed assessment.

Likewise, security measures could be based on generic assessments performed at the government level or at an organisational level or could be very specific in nature. At one extreme, security requirements might be based only on the consequences of malevolent acts without an assessment of the likelihood of the threat. A detailed threat assessment provides the means of adjusting security provisions in accordance with the results of that analysis and more specifically for addressing the potential consequences associated with loss of control over each specific source. A detailed DBT assessment methodology to define the appropriate level of security would consist of the following activities:

(i) Characterise the source, its type, nature and application (identify the target).

(ii) Perform an assessment of the potential threat within the country as a whole, based on information from security and intelligence experts.

(iii) Evaluate the potential consequences of successful actions to acquire the source. These could range from simple theft for monetary gains to deliberate acquisition of a source and threatening to use it and cause panic or even deploying it as a radiological dispersal device (RDD).

(iv) Determine, based on the assessment of threat and potential consequences, a DBT against which the security plan should be designed and evaluated. For example, the threat assessment may range from attempts to gain access by an un-armed and un-equipped person to a major attempt by an armed and well-equipped group.

(v) Based on the above, perform a vulnerability analysis for the specific source, or sources, against this DBT.

(vi) If there is a requirement to reduce the risk associated with unauthorised access and acquisition, then first optimise existing measures and then implement the additional measures. Many of these additional measures may be in the form of just extensions or enhancement of the existing safety measures.

2.5 Dynamic Nature of Security Threat Perceptions

It has to be recognised that security threats are dynamic in nature and would vary with space and time. For example, at a given place, the security threat could be different at different times. On the other hand, at a given time, the security threat may be different in different places. It is therefore necessary that the threat perception is under constant review. If the threat perception indicates deterioration in the security situation, the licencee should

immediately prepare a revised security plan, upgrade the security level of the facility as deemed desirable, implement necessary measures, submit the revised security plan to the Competent Authority for review and implement additional measures as may be recommended by the Competent Authority. In the event that the deterioration in security situation was a short-term phenomenon and the situation has reverted back to what originally existed, the licencee could revert to the original security plan and formally inform the Competent Authority.

3. SECURITY LEVELS BASED ON CATEGORISATION OF SOURCES

3.1 Purpose of Categorising Sources

Radioactive sources with a wide range of radiation intensity are used in a variety of authorised applications in medical, industrial and research institutions. Sources with high activity, if not managed safely and securely, could cause severe deterministic effects to individuals in a short period of time. The categorisation provides an internationally harmonised basis for risk informed decision making. The categorisation is not relevant to radiation generating devices such as X-ray machines and particle accelerators. There are also certain situations where the categorisation is not applicable because of factors such as specific activity, chemical properties and half-life. For example, at a waste management facility for the disposal of disused sources, the security requirements would be different from what was required when the sources were originally in use. The categorisation described in this safety guide essentially reflects the system of categorisation of sources devised by the International Atomic Energy Agency (IAEA) [6].

3.2 Basis of Categorisation

When the activity of a source is high enough to deliver a radiation dose which would result in severe deterministic effects in the exposed individual, the source is considered as a 'dangerous source'. The activity of a source, which can deliver this dose, is termed its 'D value'. Both external and internal exposures are therefore considered in the derivation of D values. The criteria for the derivation of D values are given in **Appendix-I**. Based on the D values thus derived, sources are divided into five categories [6]. The commonly used sources and their respective categories are listed in **Appendix-II**.

3.3 Graded Approach to Security

Based on the vulnerability analysis for a specific source, an assessment can be made of the level of risk involved. This risk level would determine the security measures required to protect the source. The higher the risk, the more capabile security systems are required. This 'level' of capability can be expressed in terms of the 'performance objectives' of the security system. While the range of possible specific security measures could be quite wide, they can be described by their capability to deter, to detect and to delay unauthorised access or acquisition. This graded approach will ensure that the level of security measures in place is commensurate with the potential consequence associated with the possible breach of security with respect to that source.

3.3.1 *Security Levels Applicable to Sources*

Based on the security threat associated with radioactive sources, four security levels - A, B, C and D have been defined. It must be emphasized that these security levels do not themselves lay down the security guidelines or measures. They essentially lay down a set of objectives to be achieved, with Level A requiring the highest performance objectives. These levels provide a systematic way of categorising the graded performance objectives required to cover the range of security measures that might be needed, depending on the assessed risk. The performance objectives for the four security levels of a security system are detailed below:

(i) Security Level A : Prevent unauthorised removal of a source by timely detection and response action. Measures should be established to deter and detect unauthorised access, and acquisition of the source in a timely manner. These measures should be such as to delay acquisition until a response is possible.

(ii) Security Level B : Minimise the likelihood of unauthorised removal of a source by immediate detection without having to interrupt the act. Measures should be established to deter and detect unauthorised access, and acquisition of the source in a timely manner.

(iii) Security Level C : Reduce the likelihood of unauthorised removal of a source. Measures should be established to deter unauthorised access and verify the presence of the source at set intervals.

(iv) Security Level D : Measures should be established to ensure safe use of the source and adequately protect it as an asset, verifying its presence at set intervals.

The quality and effectiveness of the security measures would be dictated by the specific design basis threat (DBT). Protection against unauthorised access for security reasons is primarily aimed at trying to prevent theft of the material. Measures to achieve this objective may already be in place arising out of safety consideration to protect against unintentional radiation exposure.

3.3.2 *Assignment of Security Level to a Radioactive Source*

The security level for a radioactive source is assigned on the basis of consequences of the perceived threat. This allows flexibility and specificity to account for the variability in threat levels and security environments. It also permits different choices of security levels for sources in the different stages of their life cycle. In the event that insufficient data are available to perform a reasonable design basis threat assessment, or it is not considered desirable or necessary to do so, then security measures could be based upon the consequences of the malevolent acquisition and use of the source(s), and an assumed threat to the source. As mentioned earlier, the sources have been

divided into five categories, with category 1 being the most significant radioactive source. Sources in categories 1 to 3 generally have the potential of giving rise to exposure sufficient to cause severe deterministic effects if they are uncontrolled. A severe deterministic effect is one that is fatal or life threatening or results in permanent injury that decreases the quality of life. The default/desired security levels and categories assigned for various sources/ practices are given in Table 3.1 which are based on implicit assumption of a threat posed by a person or group with serious intent to acquire the source. However, different circumstances or more detailed assessments may justify assigning a higher security level than indicated in this table. For example, one reason for doing this is that a specific threat assessment may reveal a facility with several sources or mobile sources to be more vulnerable, even though they may not be individually high activity sources, which may otherwise warrant a lower security level.

TABLE 3.1 : SECURITY LEVELS BASED ON CATEGORISATION OF SOURCES

Security level	Source category	Examples of practices
A	1	Radioisotope thermoelectric generators (RTGs) Irradiators Teletherapy Fixed multibeam teletherapy (gamma knife)
B	2	Industrial radiography High/medium dose rate brachytherapy
C	3	Fixed industrial gauges incorporate high activity sources (e.g. level, dredger, conveyor) Well logging gauges
D	4	Low dose rate brachytherapy (except those given against Category 5) Industrial gauges that do not incorporate high activity sources [e.g. Thickness/fill-level gauges, portable gauges (e.g. moisture/density)] Bone densitometers Static eliminators Diagnostic isotope generators
	5	Low dose rate brachytherapy eye plaques and permanent implant sources (Positron emission tomography (PET) check sources, X-ray fluorescence (XRF) devices, Electron capture devices, Mossbauer spectrometry sources) Radiopharmaceuticals and other unsealed sources

In respect of practices not included in this table, users should seek advice from the Competent Authority on the applicable security levels. Unsealed sources are assigned Security Level D in view of the activities handled and the associated potential hazard. Decayed sources are generally assigned the same security level as originally assigned to them.

3.4 Security Levels and Security Objectives

The objectives of the security functions, viz., detect, delay, response and security management apply differently to the different security levels. The detailed performance objectives against various security functions for each security level are given in **Appendix-III**. Security Level D corresponds to prudent security objectives that would be applicable to all facilities.

As emphasised earlier, it must be noted that the security level determines the specific security measures that will meet the performance objectives for that level. These security measures are described in section 4.

4. SECURITY MEASURES FOR RADIATION FACILITIES

The performance objectives for different security levels can be met by a combination of administrative and technical measures. These security measures should be seen as an integrated concept of safety and security involving industrial safety arrangements, radiation protection measures and appropriate design to achieve the necessary level of protection against unauthorised acquisition of radioactive sources.

4.1 Administrative Measures

Administrative measures are the use of policies, procedures, and practices which direct personnel to securely and safely manage sources. Administrative measures are used to support or supplement technical measures. Among others, administrative measures would include:

(i) access control procedures [e.g. personal identification number (PIN) or biometric features to activate a door control reader or a badge system which may also activate an electronic reader];

(ii) intrusion alarms at access points (e.g. with radiation detectors);

(iii) key control procedures;

(iv) video cameras or personal surveillance supported by adequate area lighting systems (even if surveillance measures involve the use of intrusion detectors instead of human observation, they are still considered as administrative measures since they do not provide a physical barrier.);

(v) records related to management of sources;

(vi) inventories;

(vii) reliability and trustworthiness of personnel;

(viii) preparation of emergency plans to respond to the loss of control of higher risk radioactive sources and carrying out exercises (the envisaged scenarios including a suspected or threatened malicious act, or a public demonstration which has the potential to threaten the security of sources or an intrusion into the security area by unauthorised persons with violent and malicious intent);

(ix) information security (protecting the confidentiality of information, the unauthorised disclosure of which could compromise the security measures, e.g. information relating to the specific location and inventory of sources, the relevant security plan and detailed security arrangements, security systems like intruder alarms, weaknesses in the security arrangements, means of response to a breach of security,

planned dates, routes and mode of transport/ shipment or transfer of sources);

(x) quality assurance measures; and

(xi) establishment and maintenance of a safety culture and a security culture.

The extent to which the above measures would need to be implemented would depend upon the security level applicable to the practice.

4.2 Technical Measures

Technical measures pose a physical barrier to the radioactive source, device or facility in order to prevent inadvertent or unauthorised access, to deter, or to prevent removal of a radioactive source. The design of technical measures and the level of quality assurance should be appropriate to the threat and the potential consequences of the defined malevolent act.

Technical measures generally comprise hardware or security devices and would include among others:

(a) fences,

(b) walls, rooms/vaults,

(c) cages,

(d) transport packaging,

(e) locks and interlocks for doors with alarm systems, and

(f) intrusion-resistant source-holding devices.

The extent to which these measures would need to be implemented would depend upon the security level applicable to the practice.

The description of security measures are given in **Appendix-IV**

4.3 Physical Protection Systems (PPS)

This term applies to the entire range of systems and equipment, which physically protect the radioactive source or the facility using a radioactive source. The design of these systems is governed by physical protection principles and physical protection can be effectively implemented through human actions supported by equipment. An effective physical protection system makes a judicious combination of human surveillance and physical protection equipment. Its design and evaluation involve concepts of DBT and vulnerability assessment (VA). **Appendix-V** gives details on PPS, which covers these aspects and could be used as a guide to develop an effective security plan.

4.4 Security of Radioactive Sources during their Transport

A radioactive source could be in storage at the facility or in use there. It could also be in transport either from the supplier of the source to the facility, or from one location to another for operational reasons, or the source is being sent to a disposal facility. As mentioned earlier, transport of a radioactive source needs special consideration from the view of safety and security. The guidance for this purpose are available separately in the AERB safety guide No. AERB/NRF-TS/SG-10 [7] and these should be used by the licencee whenever the source is in transport.

4.5 Measures Common to Security Levels A and B

There are several measures, which are common to achieve the performance objectives of Security Levels A and B. These are outlined in the following paragraphs:

4.5.1 *Availability of Formal Security Plans*

Formal security plan should be prepared for facilities possessing Category-1 sources, got duly registered with District Law and Enforcement Authority and submitted to Competent Authority for review. The specimen format for registration of security plan is given is **Appendix-VI**. For facility possessing sources of category 2 to 5, the security plan should be submitted to competent authority for review. This plan should describe how the security provisions in this document are met for the source(s) under consideration. It should be reviewed at least annually to ensure that it is still current and applicable. **Appendix-VII** outlines some of the issues that should be considered in a security plan. Security systems are effective only if they are fully implemented and are periodically tested and evaluated. System evaluations should be performed and documented as part of a quality assurance system. Whenever any component of the security system has been compromised, steps should be taken to suitably rectify the system. Towards this, there should mechanisms to detect any attempt to tamper the security system.

4.5.2 *Ensuring Security of Critical Information*

Ensuring information security is a critical factor for any security plan. Particular attention should be paid to this aspect. The 'need to know' principle should be adopted in the dissemination of such information and the distribution of relevant documents has to be controlled. Information, in this regard, applies to those pertaining to source locations, specific security measures or weaknesses in the licencee's system of management of sources, etc. Typically, this would include:

(a) specific locations of sources;

(b) the facility's security plan and security system associated with the sources;

(c) temporary or permanent weaknesses in the security system;

(d) source utilization plans and records;

(e) proposed date and time of source(s) shipment or transfer; and

(f) emergency response plans and systems.

4.5.3 *Background Checks on Key Personnel*

The licencee should ensure that persons engaged in the management of the source have a high degree of trustworthiness. This has to be established by checking the antecedents of such personnel by District Authority prior to obtaining the licence from the Competent Authority. Other personnel with access to these sources do not necessarily need such background checks as long as they are appropriately escorted or kept under visual surveillance by persons who have undergone background checks.

4.5.4 *Response to an Increased Threat Perception*

The planning for response to an increased threat involving the possible malevolent use of the radioactive source should include the role of concerned public authorities/functionaries. For example, the licencee should establish pre-arranged procedures with law and enforcement authorities regarding intelligence information and use of secure communications as well as the reactions to an increased threat.

If the licencee becomes aware, or suspects that there is a specific threat targeting a source or source storage location, the security should be increased in accordance with the threat. The increased security measures should be continued until such time as it is determined that the specific threat is no longer present. Under such circumstances, the following measures should be considered:

(a) if the source is in use, return the source to its secure storage location;

(b) preferably to have armed guards in round the clock shift as a good deterrence for Category-1 sources after evaluation of the threat levels;

(c) use video observation, or an intrusion alarm;

(d) ensure that the law and enforcement and regulatory authorities are made aware of the suspected threat;

(e) review the security procedures, facility layout, and radiation safety practices with the law enforcement and emergency response personnel; and

(f) make sure that emergency response procedures are in place. In addition, identify the nearest medical facilities where personnel trained and equipped to handle radiological emergencies are available.

4.5.5 *Availability of Emergency Response Plans*

Depending upon the magnitude and number of sources at a facility, specific emergency response procedures should be developed by the licencee. As a minimum, these would normally include informing the local police and the Competent Authority in the event of a loss of the source and the initial measures that would be made to recover lost or stolen sources. These emergency response procedures should be periodically exercised and evaluated.

4.6 Additional Measures Required for Security Level A

The performance objectives of security measures for Security Level A are to prevent unauthorised access and detect unauthorised access and acquisition of the source in a timely manner. These measures should be such as to delay acquisition until response is possible. Ideally, the access control to the source should incorporate at least two technical measures. However, it is recognised that during normal use it may not be practicable to have all these measures in place all the time. In any given situation, the quality of these security measures should be consistent with the DBT. Any unauthorised access to the source should be detected in a timely manner. The source should be accounted for on a daily basis.

Depending on whether the radioactive source is in storage or in use, following are the security measures that should be in place for Security Level A.

4.6.1 *Source in Storage*

To achieve the defined performance objective, the following security provisions could be implemented:

(a) A locked and fixed container or a device holding the source

(b) A locked storage room, separating the container from unauthorised personnel

(c) Access control to the storage room

(d) Detection of unauthorised access or removal of the source

(e) Ability to respond in a timely manner to such detection.

For a mobile device containing a high activity source, the requirements could be:

(a) Storage in a locked and shielded container

(b) Container being kept in an enclosed, secured vehicle

(c) The vehicle itself being parked inside a locked compound or locked garage

(d) The vehicle being subjected to continuous surveillance to detect intrusion attempts along with the capability to respond to any such attempt.

These measures should provide the desired degree of delay against the defined threat. Depending on the specifics of a particular threat assessment, additional responses might be required.

4.6.2 *Source in Use*

To achieve the defined performance objective, the following security provisions should be implemented :

(a) A locked device in a controlled area, separating the container from unauthorised personnel

(b) Access control to the area

(c) The room, where the source is being used, being subjected to continuous surveillance (either by personnel surveillance or electronic equipment) to detect any intrusion attempt

(d) The building housing the facility having security guards who are able to provide a timely response.

These measures should provide the desired delay against the defined threat. Depending on the assessment of the threat, additional response might be required. The above measures would be applicable by default, for example to the use of a teletherapy source in a hospital.

For a mobile source being used in the field, it might not always be possible to achieve the specified requirements. Therefore, compensatory measures, such as rigorous personnel surveillance, must be implemented. In addition, the required security measures should be re-established as soon as possible.

4.6.3 *Summary of Security Measures for Security Level A*

Table 4.1 below provides a summary of the security measures required to meet the security objectives of Security Level A :

TABLE 4.1 : SUMMARY OF SECURITY MEASURES FOR SECURITY LEVEL A

Security functions	Security objectives	Security measures
Detect	Provide immediate detection of unauthorised access to the secured area / source location	Electronic intrusion detection system and/or continuous surveillance by operating personnel
	Provide immediate detection of any attempted unauthorised removal of the source	Electronic tamper detection equipment and/or continuous surveillance by operating personnel and radiation zone monitors at the exit points.
	Provide immediate assessment of detection	Remote monitoring of CCTV or assessment by operator / response personnel
	Provide immediate communication to response personnel	Rapid, dependable diverse means of communication such as phones, cell phones, pagers, radio links, etc.
	Provide a means to detect loss through verification	Daily checking through physical checks, CCTV, tamper indicating devices, etc.
Delay	Provide delay after detection sufficient for response personnel to interrupt the unauthorised removal	System of at least two layers of barriers (e.g. walls, cages) which together provide delay sufficient to enable response personnel to interdict
Response	Respond to assessed alarm in time and with sufficient resources to interrupt and prevent the unauthorised removal	Capability for timely response with size, equipment and training to interdict
Security management	Provide access controls to source location that permits access to authorised persons only	Identification and verification, e.g. lock controlled by swipe card reader and personal identification number, or key and key control

TABLE 4.1 : SUMMARY OF SECURITY MEASURES FOR SECURITY LEVEL A (Contd.)

Security functions	Security objectives	Security measures
Security management (Contd.)	Ensure trustworthiness for individuals involved in the management of sources	Background checks for all personnel authorised for unescorted access to the source location and access to sensitive information
	Identify and protect sensitive information	Procedures to identify sensitive information and protect it from unauthorised disclosure
	Provide a security plan.	A security plan which conforms to regulatory requirements and provides for response to increased threat levels
	Ensure a capability to manage security events covered by security contingency plans	Procedures for responding to security-related scenarios
	Establish security related event report system	Procedures for timely reporting of security related events

4.7 Additional Measures Required for Security Level B

The performance objectives of security measures for Security Level B are to detect and deter any unauthorised access and acquisition of the source, in a timely manner. Ideally, there should be at least two security measures to deter any unauthorised access, with at least one of the measures being a technical one. It is recognised that it may not be practicable to have these measures in place all the time. Access controls should also be established. Any unauthorised access to the source should be detected in a timely manner and the source itself should be accounted for on a weekly basis.

Depending on whether the radioactive source is in storage or in use, following are the security measures that should be in place for Security Level B:

4.7.1 *Source in Storage*

To achieve the defined performance objective, the following security provisions could be implemented:

(a) A locked and fixed container or a device holding the source

(b) A locked storage room to separate the container from unauthorised access

(c) Access control to the room

(d) Ability to detect unauthorised access to, or removal of the source

(e) Provision of tracking mechanism on devices containing sources.

4.7.2 *Source in Use*

To achieve the defined performance objective, the following security provisions could be implemented :

(a) Use of the source in a locked room or controlled area

(b) Continuous surveillance of the source

(c) Access control to the room or controlled area.

For a mobile source, it might not always be practicable to have all the measures in place all the time. Therefore, administrative measures such as personnel surveillance need to be rigorously maintained. Compensatory measures should also be considered to provide other levels of protection. These could include, for example, establishing a communication link to allow response to incidents, or potential threats. In addition, necessary measures should be re-established as soon as possible after use.

4.7.3 *Summary of Security Measures for Security Level B*

Table 4.2 below provides a summary of the security measures required for Security Level B.

TABLE 4.2 : SUMMARY OF SECURITY MEASURES FOR SECURITY LEVEL B

Security functions	**Security objectives**	**Security measures**
Detect	Provide immediate detection of unauthorised access to the secured area/source location	Electronic intrusion detection system and/or continuous surveillance by operating personnel
	Provide immediate detection of any attempted unauthorised removal of the source	Tamper detection equipment and/or continuous surveillance by operating personnel and radiation zone monitors at the exit points

TABLE 4.2 : SUMMARY OF SECURITY MEASURES FOR SECURITY LEVEL B (Contd.)

Security functions	Security objectives	Security measures
Detect (Contd.)	Provide immediate assessment of detection	Remote monitoring of CCTV or assessment by operator/response personnel
	Provide immediate communication to response personnel	Rapid, dependable means of communication such as phones, cell phones, pagers, radio links etc.
	Provide a means to detect loss through verification	Weekly checking through physical checks, tamper indicating devices, etc.
Delay	Provide delay after detection sufficient for response personnel to interrupt the unauthorised removal	System of at least two layers of barriers (e.g. walls, cages)
Response	Provide immediate initiation of response	Equipment and procedures to immediately initiate response
Security management	Provide access controls to source location that permits access to authorised persons only	One identification measure
	Ensure trustworthiness for individuals involved in the management of sources	Background checks for all personnel authorised for unescorted access to the source location and access to sensitive information
	Identify and protect sensitive information	Procedures to identify sensitive information and protect it from unauthorised disclosure
	Provide a security plan	A security plan which conforms to regulatory requirements and provides for response to increased threat levels
	Ensure a capability to manage security events covered by security contingency plans	Procedures for responding to security-related scenarios
	Establish security related event report system	Procedures for timely reporting of security related events

4.8 Measures Required for Security Level C

The performance objectives of security measures for Security Level C are to deter unauthorised access and to verify the presence of the sources at set intervals. The licencee should ensure that persons engaged in the management of the source are authorised. Ideally, there should be at least one technical measure to deter any unauthorised access.

Access control to the area where the source is located should be provided and the source should be accounted for every month. Generic emergency plans are considered sufficient to respond to any incidents with these sources.

Depending on whether the radioactive source is in storage or in use, following are the security measures that should be in place for Security Level C:

4.8.1 *Source in Storage*

To achieve the defined objective, Security Level C requires that the source is stored in a locked, fixed container and in a room to which the access is controlled.

4.8.2 *Source in Use*

The appropriate control on a radioactive sources which requires Security Level C, would be measures to make sure that only an authorised person uses the source and that too only in an area to which the access is controlled or to make sure that the source is in a secure containment in an area where there are personnel able to detect any interference with the source.

4.8.3 *Summary of Security Measures for Security Level C*

Table 4.3 below provides a summary of the security measures required for Security Level C.

TABLE 4.3 : SUMMARY OF SECURITY MEASURES FOR SECURITY LEVEL C

Security functions	Security objectives	Security measures
Detect	Provide immediate detection of any attempted unauthorised removal of the source	Tamper detection equipment and/ or continuous surveillance by operating personnel
	Provide immediate assessment of detection	Assessment by operator/response personnel
	Provide a means to detect loss through verification	Monthly checking through physical checks, tamper indicating devices, etc.
Delay	Impede the unauthorised removal	One barrier (e.g. cage, source housing) or under observation by operating personnel
Response	Implement appropriate action in the event of unauthorised removal of source	Procedures for identifying necessary action in accordance with contingency plans
Security management	Provide access controls to source location that permits access to authorised persons only	One identification measure
	Ensure trustworthiness for individuals involved in the management of sources	Background checks for all personnel authorised for unescorted access to the source location and access to sensitive information
	Identify and protect sensitive information	Procedures to identify sensitive information and protect it from unauthorised disclosure
	Provide a security plan	A security plan which conforms to regulatory requirements and provides for response to increased threat levels
	Ensure a capability to manage security events covered by security contingency plans	Procedures for responding to security-related scenarios
	Establish security related event report system	Procedures for timely reporting of security related events

4.9 Measures Required for Security Level D

The performance objectives of security measures for Security Level D are to ensure safe use of the source, to adequately protect it as an asset and verify its presence at periodic intervals of once in three months. The personnel in charge of managing sources requiring Security Level D should be formally approved as authorised personnel by the management. The source should be protected by application of the relevant safety standards as well as appropriate industrial standards. The natural interest of the owner to protect the asset and to ensure safe use and storage is considered as an appropriate basis for this security level.

4.10 Security for Aggregation of Sources

In general, the security measures given in this section are intended for implementation with regard to security of individual sources. The categorisation of radioactive sources described in section 3 incorporates a method for appropriately categorising aggregations of sources at a given location. Hence, it would be sufficient if Table 3.1 is used as the basis of determining the applicable level of security. However, when there is an aggregation of sources, the security level should be appropriately upgraded depending upon the types of sources, their number and their activity. Accumulation of decayed/disused sources at a facility, pending disposal, is an instance of aggregation of sources.

4.11 Temporary Storage of Recovered Sources

A source is considered to be in temporary storage when the licencee or any other responsible authority is actively seeking a permanent storage for the source or its transfer to another authorised agency. A source in temporary storage should be transferred to a designated facility as soon as practicable. For the duration of the temporary storage of such sources, the security level applicable to the radiation facility should be determined and the appropriate security measures implemented. Examples of such situations when the need for temporary storage could arise are those following an emergency or following the discovery of an orphan source or after the recovery of a stolen source.

4.12 Preparation and Submission of Security Plan to Competent Authority

Based on the guidance give in this section, the licencee should prepare a security plan for the facility using the radioactive source. The comprehensiveness of this plan would obviously depend on the security level assigned to the application or use of the radioactive source as identified in Table 3.1. In this regard, a summary of the security measures required to meet the performance objectives under Security Levels A to D is given in Table 4.4 below:

TABLE 4.4 : SUMMARY OF SECURITY MEASURES TO BE CONSIDERED

Security Level A	Security Level B	Security Level C	Security Level D
General administrative measures	General administrative measures	General administrative measures	General administrative measures
Daily accounting	Weekly accounting	Monthly accounting	Quarterly accounting
Access control to source location allowing timely detection of unauthorised access	Access control to source location allowing timely detection of unauthorised access	Access control to source location	No specific provisions. Routine measures to ensure safe use and protect as an asset
Deterrence provided by : Two technical measures separating the source from unauthorised personnel	Deterrence provided by : Two measures (one technical) separating the source from unauthorised personnel	Deterrence provided by : One technical measure separating the source from unauthorised personnel	
Specific emergency response plan	Specific emergency response plan	Generic emergency response plan	
Background checks			
Security plan			
Information security			
Upgrade security for increased threat			
Timely detection provided by : Remotely monitored intruder alarm	Timely detection provided by : Local alarm		
Timely response to an alarm			

To facilitate the licencee in preparing the appropriate security plan, security guidelines for typical applications, are given in **Appendices-VIII to XI**. These guidelines are by no means comprehensive. The licencee should draw up the security plan specific to the radiation facility on the basis of their threat assessments and the security needs.

The security plan prepared using the guidelines detailed above, should be formally submitted by the Licencee to the Competent Authority for review.

5. RESPONSIBILITIES

5.1 General

It is now a well recognised concept that just like safety and quality, security is a matter of common interest to the entire organisation and cannot be the responsibility of any one agency. Because of the safety implications of a security breach, it is essential that all the employees at a radiation facility have to be sensitised of their respective roles in ensuring security of the radioactive sources used at that facility. Persons working in a radiation facility such as employer, licencee, RSO and all others involved in handling the radioactive material, should implement the security measures dentified as part of their responsibilities in the security plan. The present security scenario also necessitates that government agencies dealing with law and order have a major role in preventing breach of security of radioactive sources as such breach may undermine or even jeopardize public safety. The Competent Authority may impose penalties for non-compliance with the security requirements by the licencee.

Contingency plans to respond to malicious acts involving radioactive sources including the recovery of lost or stolen material and for mitigation of consequences, should be established in advance by the licencee, concerned emergency response organisations and by the law enforcing authority.

5.2 Radiation Facility

The security related responsibilities of the employer, the licencee, the radiological safety officer (RSO), the workers occupationally exposed to radiation, other personnel working in a radiation facility and the security personnel are broadly described in the following paragraphs.

5.2.1 *Employer*

As the owner of the facility using a radioactive source, the employer has the primary responsibility for ensuring and maintaining the safety and the security of the sources. This guide outlines guidance for preparing the appropriate security plan for the facility, which has to be submitted to the Competent Authority for review. In this regard, the employer is primarily responsible for ensuring that the security plan at the facility is implemented in letter and spirit. In particular, the employer is responsible for:

(i) ensuring that all personnel and their contract workers who use or have access to the sources are reliable;

(ii) reporting to the Competent Authority of a source in the facility, provide the origin and/or identity of which cannot be established;

(iii) promoting a security culture and establishing a management system commensurate with the security needs to ensure that problems affecting security are promptly identified and corrected, clear lines of authority are defined for security related decision making and sensitive information is identified and protected on a 'need to know' basis; and

(iv) promptly responding to any request from the local law enforcing authorities in the recovery of any lost or stolen source.

5.2.2 *Licencee*

As the individual who is responsible for preparing a security plan and submitting to the Competent Authority and obtaining the licence in his/her name, the Licencee has a major responsibility in ensuring the security of the radioactive sources at the facility. The Licencee's responsibility commences from the moment the authorised radioactive material is received in the radiation facility. In particular, the Licencee should ensure that the following actions are carried out:

(i) Assess the security threats, evaluate the security requirements, design the security provisions and prepare a security plan for the facility in consultation with the security personnel.

(ii) Implement the security plan along with its administrative and technical measures to ensure the safety and security of the radioactive sources at the facility.

(iii) Bring to the notice of the Employer any additional actions specified by the Competent Authority, for implementation.

(iv) Establish a specific security clearance procedure for those persons in the radiation facility who would be involved in the use of the source, as also those personnel who would be deputed to collect the source from the supplier or carrier on behalf of the facility.

(v) Procure radioactive material only from an authorised supplier.

(vi) Maintain a complete inventory of all sources in the facility.

(vii) Ensure that the storage of a source not in use, its transfer to any other person/agency is done in accordance with procedures and requirements prescribed by the Competent Authority.

(viii) Promptly respond to any request from the local law enforcing authorities in the recovery of any lost or stolen source.

(ix) Submission of reports to the Competent Authority at prescribed intervals in the prescribed format, on the status relating to the safety and security of sources handled in the facility. This should include

any unusual events that have a bearing on the security of the sources and would include among others, loss of control, unauthorised access, unauthorised use, malicious acts threatening the authorised activities, failures of equipment containing sources which may have security implications and discovery of any unaccounted source.

(x) Any attempt to or actual breach of security including attempted thefts and actual thefts, and even misplacement or loss of radioactive material or loss/theft of sensitive information is reported to the law enforcing authorities and the Competent Authority within 24 hours of the event.

5.2.3 *Radiological Safety Officer (RSO)*

While the RSO's primary responsibility is to implement radiological safety requirements at the facility, he / she should be fully aware of the fact that any breach of security has safety implications. Consequently, with regard to ensuring security of radioactive sources, the RSO should:

(i) ensure that persons entering the area/zone where a radioactive source is used/or in use, have been permitted by the Concerned Authority;

(ii) implement when required, the procedure for mitigating the consequences of a breach of security;

(iii) inform and train all the personnel working with radiation in the facility and other personnel as well about the safety and security of sources;

(iv) secure the records appropriately and update the routine source inventory. This should also include source use history;

(v) bring to the notice of the licencee, the employer and the security personnel of the facility, any situation which could be a potential threat to the security of source(s) in the facility.

5.2.4 *Workers and Other Personnel*

Persons occupationally exposed to radiation in a facility and the other workers should implement the procedure relating to the security of sources in the facility. If they detect any threat to the safety and security of the sources handled in the facility they should immediately report the matter to the RSO, the licencee, the employer and the security personnel of the facility.

5.2.5 *Security Personnel*

The security personnel of the facility should obtain the relevant information about the sources handled in the facility and provide the necessary advice, guidance and co-operation in devising and implementing the security plan of the radiation facility.

5.3 Supplier of the Source

The source supplier should possess a licence from the Competent Authority (Chairman, AERB) to supply radioactive material as required in the Atomic Energy (Radiation Protection) Rules, 2004 and should further ensure that the radioactive material is being supplied only to the person authorised to receive and handle the source. Further, appropriate security measures should be implemented in the supplier's facility on the basis of an approved security plan. The responsibilities of the employer, licencee, RSO, workers and other personnel including the security personnel should be identified in the security plan.

5.4 Role of Law and Enforcement Agencies

The government agencies dealing with law and enforcement constantly review the prevailing security scenario and communicate the necessary warnings/ alerts/advisories about perceived security threats, sufficiently in advance to the concerned agencies. The licencee is required to work out a coordination mechanism with the concerned law and enforcement agencies as mentioned in this document to ensure that the facility using the radioactive source gets these warnings/alerts/advisories in time so that appropriate security measures could be implemented. The threat assessment process adopted by the law and enforcement authority would generally be based on their knowledge of the characteristics of the potential offender(s), who may be an internal or an external adversary. The law and enforcement authority is also expected to extend the necessary support in the event of a theft of a source. Where necessary, police protection should be available to personnel investigating cases of theft of a source.

APPENDIX-I

DOSE CRITERIA USED IN THE DERIVATION OF THE D VALUES

Categorisation of the sources is based on the D value of the source as stated in section 3. The D values are determined on the basis of certain dose criteria, which are given below:

(i) A dose of 1 Gy to the bone marrow or 6 Gy to the lung from low linear energy transfer (LET) radiation, received by the organ in 2 d.

(ii) A dose of 25 Gy to the lung from inhalation exposure to high LET radiation in 1 year. This is the dose level at which fatalities are likely to be induced within 1.5 years.

(iii) A dose of 5 Gy to the thyroid received by the organ in 2 d. This is the dose level at which intervention is justified to prevent hypothyroidism.

(iv) For a source in contact with tissue, a dose of more than 25 Gy at a depth of (i) 2 cm for most parts of the body (e.g. from a source in a pocket) or (ii) 1 cm for the hand for a period of 10 h. This is the threshold dose for necrosis.

(v) For a source that is considered too big to be carried, a dose of 1 Gy to the bone marrow in 100 h from a source at a distance of 1 m.

In summary, the reference doses for D values are given in the table below:

TABLE I-1 : REFERENCE DOSES FOR D VALUES

Tissue	Dose criteria
Bone marrow	1 Gy in 2 d for a source that can be carried by an individual 1 Gy in 100 h for a source that is too big to be carried
Lung	6 Gy in 2 d from low LET radiation 25 Gy in 1 year from high LET radiation
Thyroid	5 Gy in 2 d
Skin/tissue (contact)	25 Gy at a depth of 2 cm for most parts of the body (e.g. from a source in a pocket) or 1 cm for the hand, for a period of 10 h

The D values derived for some of the commonly used sources are given in Table I-2.

TABLE I-2 : ACTIVITY CORRESPONDING TO A DANGEROUS SOURCE (D VALUE)[a] FOR SELECTED RADIONUCLIDES

S. No.	Radionuclide	D value (TBq)	S.No.	Radionuclide	D value (TBq)
1.	Am-241	6.E-02	18.	Mo-99	3.E-01
2.	Am-241/Be	6.E-02	19.	Ni-63	6.E+01
3.	Au-198	2.E-01	20.	P-32	1.E+01
4.	Cd-109	2.E+01	21.	Pd-103	9.E+01
5.	Cf-252	2.E-02	22.	Pm-147	4.E+01
6.	Cm-244	5.E-02	23.	Po-210	6.E-02
7.	Co-57	7.E-01	24.	Pu-238	6.E-02
8.	Co-60	3.E-02	25.	Pu-239[b]/Be	6.E-02
9.	Cs-137	1.E-01	26.	Ra-226	4.E-02
10.	Fe-55	8.E+02	27.	Ru-106 (Rh-106)	3.E-01
11.	Gd-153	1.E+00	28.	Se-75	2.E-01
12.	Ge-68	7.E-01	29.	Sr-90 (Y-90)	1.E+00
13.	H-3	2.E+03	30.	Sr-90	1.E+00
14.	I-125	2.E-01	31.	Tl-204	2.E+01
15.	I-131	2.E-01	32.	Tm-170	2.E+01
16.	Ir-192	8.E-02	33.	Tc-99m	7.E-01
17.	Kr-85	3.E+01	34.	Yb-169	3.E-01

a Since this Table does not show which dose criteria were used, these D values should not be used in reverse to derive possible doses due to sources of known activity.

b Criticality and safeguards issues will need to be considered for large multiples of D.

On the basis of the above discussion, sources used in the various applications are categorised as given in Table I-3 below:

TABLE I-3 : CATEGORISATION OF SOURCES USED IN DIFFERENT APPLICATIONS

Category	Source[a] and practice	Activity ratio[b]
1	Radioisotope thermoelectric generators (RTG) Irradiators Teletherapy sources Fixed multibeam teletherapy (gamma knife)	$A/D \geq 1000$
2	Industrial gamma radiography High/medium dose rate brachytherapy	$1000 > A/D \geq 10$
3	Fixed industrial gauges that incorporate high activity sources (e.g. level, dredger, conveyor gauges) Well logging gauges Sources used in the blast furnace lining Calibration sources Research reactor startup sources Sources used in pacemakers (^{238}Pu)	$10 > A/D \geq 1$
4	Low dose rate brachytherapy (except eye plaques and permanent implant sources) Industrial gauges that do not incorporate high activity sources [e.g. Thickness/fill-level gauges, portable gauges (e.g. moisture/density gauges)] Low activity calibration sources (e.g. ^{90}Sr :74 GBq) Bone densitometers Static eliminators Diagnostic isotope generators	$1 > A/D \geq 0.01$
5	Low dose rate brachytherapy eye plaques and permanent implant sources Positron emission tomography (PET) check sources X ray fluorescence (XRF) devices Electron capture devices Mossbauer spectrometry sources Radiopharmaceuticals and other unsealed sources	$0.01 > A/D$ and $A \geq \text{Exempt}^{c} / D$

Foot notes:

a In addition to the A/D ratio other factors like, the nature of the work with the source, the mobility of the source experience from reported accidents and typical and unique activities within an application have been taken into consideration.

b This column can be used to determine the category of a source, based purely on A/D. This may be appropriate if, for example, the practice is not known or is not listed; sources have a short half-life and/or are unsealed; or sources are aggregated.

i.e. Aggregate $A/D = \Sigma_n \ (\Sigma_i \ A_{i,n}/D_n)$

where, $A_{i,n}$ = activity of each individual source 'i' of radionuclide 'n' in the aggregation of sources; and D_n = D value for radionuclide 'n'.

This principle will apply to situations in which radioactive sources are in close proximity to each other in the same room or building, such as in a source manufacturer's facility or in a storage facility.

c Exempt quantities as notified under the Atomic Energy (Radiation Protection) Rules, 2004.

The above source categorisation is an important consideration in the evaluation of the security requirements and the design of security provisions which should be carried out by the licencee.

APPENDIX-II

CATEGORIES OF COMMONLY USED SOURCES

A list of sources used in some common practices, the quantities in which they are generally handled and also their D values and the respective categories of the sources are listed in the table below:

CATEGORIES FOR SOURCES USED IN SOME COMMON PRACTICES

(There may be certain cases where the activity of the sources handled could exceed the values indicated)

Source	Activity handled (A) (TBq)	D value (TBq)	Ratio of A/D
Category 1			
RTGs			
Sr-90	2.5E+04	1.0E+00	2.5E+04
Pu-238	1.0E+01	6.E-02	1.7E+02
Irradiators used in sterilisation and food preservation			
Co-60	5.6E+05	3.E-02	1.9E+07
Cs-137	1.9E+05	1.E-01	1.9E+06
Self-shielded irradiators			
Cs-137	1.6E+03	1.E-01	1.6E+04
Co-60	1.9E+03	3.E-02	6.2E+04
Blood/tissue irradiators			
Cs-137	4.4E+02	1.E-01	4.4E+03
Co-60	1.1E+02	3.E-02	3.7E+03
Multi-beam teletherapy (gamma knife) sources			
Co-60	3.7E+02	3.E-02	1.2E+04
Teletherapy sources			
Co-60	5.6E+02	3.E-02	1.9E+04
Cs-137	5.6E+01	1.E-01	5.6E+02

Source	Activity handled (A) (TBq)	D value (TBq)	Ratio of A/D
Category 2			
Industrial radiography sources			
Co-60	7.4E+00	3.E-02	2.5E+02
Ir-192	7.4E+00	8.E-02	9.3E+01
Tm-170	7.4E+00	2.E+01	3.7E-01
Yb-169	3.7E-01	3.E-01	1.2E+00
Se-75	3.0E+00	2.E-01	1.5E+01
Brachytherapy sources - high/medium dose rate			
Co-60	7.4E-01	3.E-02	2.5E+01
Cs-137	3.0E-01	1.E-01	3.0E+00
Ir-192	4.4E-01	8.E-02	5.6E+00
Calibration sources			
Co-60	1.2E+00	3.E-02	4.1E+01
Cs-137	1.1E+02	1.E-01	1.1E+03
Category 3			
Level gauges			
Cs-137	1.9E-01	1.E-01	1.9E+00
Co-60	3.7E-01	3.E-02	1.2E+01
Conveyor gauges			
Cs-137	1.5E+00	1.E-01	1.5E+01
Cf-252	1.4E-03	2.E-02	6.8E-02
Blast furnace gauges			
Co-60	7.4E-02	3.E-02	2.5E+00
Dredger gauges			
Co-60	9.6E-02	3.E-02	3.2E+00
Cs-137	3.7E-01	1.E-01	3.7E+00
Research reactor startup sources			
Am-241/Be	1.9E-01	6.E-02	3.1E+00
Well logging sources			
Am-241/Be	8.5E-01	6.E-02	1.4E+01
Cs-137	7.4E-02	1.E-01	7.4E-01
Cf-252	4.1E-03	2.E-02	2.0E-01

Source	Activity handled (A) (TBq)	D value (TBq)	Ratio of A/D
Category 3 (Contd.)			
Pacemakers			
Pu-238	3.0E-01	6.E-02	4.9E+00
Calibration sources			
Pu-239/Be	3.7E-01	6.E-02	6.2E+00
Am-241	7.4E-01	6.E-02	1.2E+01
Category 4			
Brachytherapy sources - low dose rate			
Cs-137	2.6E-02	1.E-01	2.6E-01
Ra-226	1.9E-03	4.E-02	4.6E-02
I-125	1.5E-03	2.E-01	7.4E-03
Ir-192	2.8E-02	8.E-02	3.5E-01
Au-198	3.0E-03	2.E-01	1.5E-02
Cf-252	3.1E-03	2.E-02	1.5E-01
Thickness gauges			
Kr-85	3.7E-02	3.E+01	1.2E-03
Sr-90	7.4E-03	1.E+00	7.4E-03
Am-241	2.2E-02	6.E-02	3.7E-01
Pm-147	1.9E-03	4.E+01	4.6E-05
Cm-244	3.7E-02	5.E-02	7.4E-01
Fill level gauges			
Am-241	4.4E-03	6.E-02	7.4E-02
Cs-137	2.4E-03	1.E-01	2.4E-02
Co-60	1.9E-02	3.E-02	6.2E-01
Calibration sources			
Sr-90	7.4E-02	1.E+00	7.4E-02
Moisture detectors			
Am-241/Be	3.7E-03	6.E-02	6.2E-02
Density gauges			
Cs-137	3.7E-04	1.E-01	3.7E-03

Source	Activity handled (A) (TBq)	D value (TBq)	Ratio of A/D
Category 4 (Contd.)			
Moisture/density gauges			
Am-241/Be	3.7E-03	6.E-02	6.2E-02
Cs-137	4.1E-04	1.E-01	4.1E-03
Ra-226	1.5E-04	4.E-02	3.7E-03
Cf-252	2.6E-06	2.E-02	1.3E-04
Bone densitometry sources			
Cd-109	7.4E-04	2.E+01	3.7E-05
Gd-153	5.6E-02	1.E+00	5.6E-02
I-125	3.0E-02	2.E-01	1.5E-01
Am-241	1.0E-02	6.E-02	1.7E-01
Static eliminators			
Am-241	4.1E-03	6.E-02	6.8E-02
Po-210	4.1E-03	6.E-02	6.8E-02
Diagnostic isotope generators			
Mo-99	3.7E-01	3.E-01	1.2E+00
Medical unsealed sources			
I-131	7.4E-03	2.E-01	3.7E-02
Category 5			
XRF analyser sources			
Fe-55	5.0E-03	8.E+02	6.2E-06
Cd-109	5.6E-03	2.E+01	2.8E-04
Co-57	1.5E-03	7.E-01	2.1E-03
Electron capture detector sources			
Ni-63	7.4E-04	6.E+01	1.2E-05
H-3	1.1E-02	2.E+03	5.6E-06
Lightning preventers			
Am-241	4.8E-04	6.E-02	8.0E-03
Ra-226	3.0E-06	4.E-02	7.4E-05
H-3	7.4E-03	2.E+03	3.7E-06

Source	Activity handled (A) (TBq)	D value (TBq)	Ratio of A/D
Category 5 (Contd.)			
Brachytherapy sources: low dose rate eye plaques and permanent implants			
Sr-90	1.5E-03	1.E+00	1.5E-03
Ru/Rh-106	2.2E-05	3.E-01	7.4E-05
Pd-103	1.1E-03	9.E+01	1.2E-05
PET check sources			
Ge-68	3.7E-04	7.E-01	5.3E-04
Mossbauer spectrometry sources			
Co-57	3.7E-03	7.E-01	5.3E-03
Tritium targets			
H-3	1.1E+00	2.E+03	5.6E-04
Medical unsealed sources			
P-32	2.2E-02	1.E+01	2.2E-03

Notes:

1. Calibration sources are found in all categories except Category 1.
2. Pu- 238 sources are no longer manufactured for use in pacemakers.
3. Unsealed medical sources typically fall into Categories 4 and 5. The unsealed nature of these sources and their short half-lives require case by case categorisation.

APPENDIX-III

SECURITY LEVELS AND SECURITY OBJECTIVES

Security Functions	Security objectives		
	Security Level A (To prevent unauthorised removal)	**Security Level B** (To minimise likelihood of unauthorised removal)	**Security Level C** (To reduce likelihood of unauthorised removal)
Detect	Provide immediate detection of unauthorised access to the secured area/source location		------
	Provide immediate detection of any attempted unauthorised removal of the source		Provide detection of unauthorised removal of the source
	Provide immediate assessment of detection		
	Provide immediate communication to response personnel		
	Provide a means to detect loss through verification		
Delay	Provide delay after detection sufficient for response personnel to interrupt the unauthorised removal	Provide delay to minimise the likelihood of unauthorised removal	Impede the unauthorised removal
Response	Respond to assess alarm in time and with sufficient resources to interrupt and prevent the unauthorised removal	Provide immediate initiation of response	Implement appropriate action in the event of unauthorised removal of a source
Security management	Provide access controls to source location that permits access to authorised persons only		
	Ensure trustworthiness for individuals involved in the management of sources		
	Identify and protect sensitive information		
	Provide a security plan		
	Ensure a capability to manage security events covered by security contingency plans		
	Establish security event reporting system		

Notes:

1. It may be noted that as regards the ‘deterrence’ security function, implementing specific measures for detection, delay, response and security management would in themselves serve as a deterrent.

2. As regards Security Level D, the objectives would be achieved through adoption of standard prudent security measures, which would be adopted by any organisation to periodically verify the presence of its assets and take measures to protect the same.

APPENDIX-IV

DESCRIPTION OF SECURITY MEASURES

Recommended security measures some of which are referenced in Section 4 are described below:

IV.1 Access Control

Access control can be exercised through entry checkpoints controlled by response personnel, the use of electronic readers or key control measures. Technology, in the form of automatic access control systems (AACS), is available in various forms, from simple pushbutton mechanical devices to more sophisticated readers that respond to proximity tokens or individual biometric characteristics. In most cases, the use of a card should be verified by a PIN keyed into the reader and in high security situations an AACS entry point should be supervised by a guard positioned within view. The essential factor for prospective operators is to specify a viable AACS that is appropriate to the requirement and can be supported locally by a manufacturer or an installer. It is also important to limit access to the AACS management computers and software to prevent unauthorised interference with the system database. Where conventional lock and key are used as a means of control, locks should be of good quality and key management procedures should be designed to prevent unauthorised access or compromise.

IV.2 Cages

Metal cages or containers may also be used to segregate and secure sources by adding another level of protection, e.g. temporary retention within a receipt and dispatch area. Elsewhere, cages could be part of the storage arrangements within an established area that is enclosed, under control and supervision.

IV.3 CCTV Surveillance

CCTV is a useful aid which allows security staff to monitor outer approaches and areas where radioactive sources are stored. Cameras can be combined with an intrusion detection system (IDS) to provide event activated camera views. However, to be fully effective, the performance of CCTV cameras and monitors should be regularly assessed to ensure that they continue to display imagery of good quality. Systems should also be supported by a response so that alarm events and indications activated by technology can be investigated.

IV.4 Communication

Security personnel at all levels should be provided with effective and reliable forms of communication. This includes communication between patrols, fixed

posts and the local reporting or control centre and the communication to external agencies responsible for providing rapid response to security events.

IV.5 Fences and Gates

The type fence used on a perimeter should be appropriate to the threat, the nature of the sources being protected and the category of the site overall. There are various types of fence ranging from those that are little more than a demarcation to those that are more robust and can be combined with a fence mounted perimeter intrusion detection and assessment system or electrified panels. Fence lines need to be checked regularly to ensure that the fabric is in good order and free from interference or damage. Gates within a fence should be constructed to a comparable standard to the fence and secured with good quality locks.

IV.6 Intrusion Detection Systems (IDS)

These systems are a useful means of monitoring the security of an unoccupied area. Where appropriate, the technology can be extended to the outer area of an establishment by use of a perimeter intrusion detection and assessment system. All intrusion detection systems should be supported by a response to investigate alarm events or conditions. Alarms can sound remotely at a security control point or locally through a high volume sounder. CCTV can be a useful aid in providing initial verification of events within an alarmed zone or area but should normally be backed up by a patrol making a visual check or investigation.

IV.7 Key Control Procedures

Keys which allow access to radioactive sources should be controlled and secured. These keys may be to cages, doors, storage containers or shielded units within which sources are used. Similar levels of control should be applied to duplicate and spare keys.

IV.8 Locks, Hinges and Interlocks for Doors

Locks used for the protection of radioactive sources should be of good quality, incorporating features that will offer some resistance to forcible attack. The same applies to hinges on doors. Keys should be safeguarded in a manner outlined above under the procedural measures. Within premises, interlock doors that meet safety requirements can serve the interests of security by controlling the movement of personnel and allowing staff to monitor access to the facility.

IV.9 Locked, Shielded Containers

Shielding and fixed units containing radioactive sources can provide protection, and can delay any attempt to interfere with the source. However,

when staff members are not present, the area should be covered by an intruder detection alarm system to alert the response personnel or security response of the need to investigate the circumstances of any intrusion.

IV.10 Maintenance and Testing of Security Technology

Considerable reliance should be placed upon security technology to provide early warning of the entry of an adversary to the site or the secured area. Intruder detection systems used for the protection of the radioactive sources should therefore not only be properly specified but also tested for performance upon installation, maintained at regular intervals by competent persons, and tested at intervals specified by the regulatory body.

IV.11 Pass Systems

A pass system is an efficient and cost effective means of providing a first level indication of individual authority to be within a premises or a secured area. Nevertheless, passes should be checked on entry to the facility and worn visibly by holders to confirm authority and aid identification. Embedded technology can also allow passes to be combined with use in access control systems.

IV.12 Quality Assurance

Security arrangements and procedures should be prepared, documented and maintained in line with recommended quality assurance standard such as: recording of formal approval, version control, periodic and planned review, testing of arrangements and procedures, and incorporation of lessons learned into procedures.

IV.13 Security and Area Lighting

Effective illumination of areas can make an important contribution to physical protection. In high security situations special lighting configurations may be necessary. However, area and street lighting that may be in place for other purposes can often provide illumination to deter intruders and assist patrolling response personnel.

IV.14 Special Security Doors and Door Sets

Within certain facilities containing radioactive sources, it may be appropriate to fit storage areas with special security doors and door surrounds that offer resistance to forcible attack. This would be relevant in areas that are regularly left unattended.

IV.15 Standby Power

Security control rooms and security systems should be able to cope with power dips or outright loss of a main electric supply. This can be ensured

through an uninterruptible power supply and a standby generator which automatically starts when a fluctuation in power levels is detected. Battery backup has only limited duration and should, therefore, be viewed as a short term source of standby power.

IV.16 Walls

Unless they are already in place, walls are expensive way to form a perimeter boundary. Walls also have the disadvantage of preventing response personnel from looking out beyond the protected area.

APPENDIX-V

PHYSICAL PROTECTION SYSTEMS (PPS)

V.1 Physical Protection Principles

The design of the physical protection system (PPS) for a given source or combination of sources is mainly governed by three steps viz. assessment of security risk, establishment of performance objectives for the PPS commensurate with the security risk, and identification of a combination of security measures that meet the performance objectives. The security risk is associated with all the security levels and can be estimated by carrying out threat assessment and vulnerability analysis.

V.2 Physical Protection Equipment

Physical protection can be effectively implemented through human actions supported by equipment. Physical protection equipment include turnstile gates which will regulate the entry and exit of individuals enabling direct surveillance, entrance doors operated by electronic recognition of security cards, provision of intrusion alarms, video cameras, etc. Physical protection equipment are many and varied. An effective physical protection system makes a judicious combination of human surveillance and physical protection equipment.

V.3 Design and Evaluation of PPS

The design and evaluation of physical protection system (PPS) need to take into account the current national threat assessment and may include the development and applications of design basis threat (DBT). PPS should be such that it is effective in countering assessed threat and its security status is heightened during times of increased threat. Such an assessment is normally conducted by the Governmental Agencies such as Ministry of Home, Intelligence Bureau, Ministry of External Affairs, Law Enforcement Agencies, Customs and Coast Guard, Regulatory Authorities and other agencies with security related responsibilities. A DBT describes the attributes and helps in establishing performance requirements for the design of physical protection system for specific types of radiation facilities. The threat assessment should consider an insider threat, which could be from one or more persons and should be given particular recognition when designing the physical protection system. A DBT is a tool used to establish performance requirements for the design of physical protection systems for specific types of radiation facilities.

A DBT is used to help the employer and the licencee to assess the effectiveness of the systems to counter adversaries by evaluating the systems

performance against adversary capabilities described in the DBT, through a vulnerability assessment (VA). VA is also known as security survey or security assessment and is a method for evaluating the effectiveness of the physical protection system. The VA can be specific or general in nature, and need to be conducted by the licencee. The Competent Authority may verify the VA. The following are the essential elements of VA:

(i) Establishing a radioactive source inventory, including both used and disused sources, and associated information

(ii) Considering national threat assessment and also any local considerations

(iii) Identifying existing security measures and assessing the expected effectiveness of the PPS in protecting against attacks by postulated threat

(iv) Determining if any, additional security measures are required to ensure an acceptable and proportionate level of protection.

There can be three alternative approaches that user can apply to ensure the achievement of security objective. These are prescriptive approaches, performance based approaches and combined approaches. A prescriptive approach is based on the specific security measures, which have been established for particular category of sources (refer section 3 of this document). It establishes the level of performance of PPS that must be achieved. It considers the understanding of radiation facility in the context of security (i.e. physical attributes of devices housing sources, whether the source is in use /storage, nature of operations in which source is handled, accessibility of source during working and non working hours and mobility or portability of source), categories of sources used in it, performance objectives and designing security system to include security measures. A performance-based approach is based on the national threat (NT) assessment/DBT and allows the user to establish security measures based on vulnerability analysis. It is used to assess how a PPS performs against the DBT. It uses the principle of 'timely detection' to determine its effectiveness and then evaluate and upgrade the PPS. A combined approach includes measures drawn from both prescriptive and performance based approaches. For example, a performance based approach can be applied for the sources with the highest potential consequences of malicious use and a prescriptive approach for lower potential consequences sources.

The following security principles should be considered in designing the security system:

(i) The impact of deterrence can be quantified only by the frequency of attempted malicious acts. So the design of a security system cannot be based entirely on deterrence.

(ii) Detection should precede delay. Hence the detection systems should be installed so that the attempts to commit a malicious act such as stealing a source are detected at early stages of the attempt. Detection would be effective only with human interfacing.

(iii) The delay factor of the security system can be effective only if the delay time is greater than the time taken by the detection system plus the time required for the response actions to be activated. The combined effect of detection, delay and response is termed ‘timely detection’.

(Note: To be printed on Radiation Facility letter head)

APPENDIX-VI

SPECIMEN FORMAT FOR REGISTRATION OF SECURITY PLAN FOR CATEGORY-1 SOURCES

Sub: Proposal for registration of security plan with District Law and Enforcement Authority

As per the requirements specified in section 4.5.1 of the AERB Safety Guide on 'Security of Radioactive Sources in Radiation Facilities', (AERB/RF-RS/SG-1), published by the Atomic Energy Regulatory Board (AERB), which is the Competent Authority for radiation protection in the country, the security plan need to be registered with the District Law and Enforcement Authority. Herewith please find the details of our radiation facility along with the proposed security plan for registration.

1. Name and address of the Radiation Facility:
2. Name and Designation of Head of the Radiation Facility:
3. Contact details including Tele./Fax. and E-mail:
4. Description of the sources and their use :
5. Physical security arrangement to the Radiation Facility :
   (Copy of the security plan attached)

The District Law and Enforcement Authority is requested to kindly register our facility with your office and endorse the enclosed security plan for further submission to the Competent Authority (Atomic Energy Regulatory Board).

Signature
Name & Designation of the
Head of the Radiation Facility

<u>Official Use by District Law and Enforcement Authority</u>

The above radiation facility has been registered with our office and the copy of the security plan is reviewed by us and same is endorsed for further action by the Competent Authority (AERB).

Authorised Signatory

District Law and Enforcement Authority

(Seal with date)

APPENDIX-VII

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
- (ii) 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

APPENDIX-VIII

GUIDELINES TO PREPARE SECURITY PLAN FOR GAMMA IRRADIATOR FACILITY/TELETHERAPY FACILITY (SOURCE CATEGORY 1 AND SECURITY LEVEL A)

The security plan should be prepared addressing the issues in **Appendix-VII**. 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:	Electronic tamper detection equipment and/or continuous surveillance by operating personnel. During source replacement, special care should be taken.
3.	Security objective:	Provide immediate assessment of detection.
	Security measures:	Remote monitoring of CCTV or assessment by operator/response personnel. Any significant change in the ambient radiation level should be treated as an alert signal.
4.	Security objective:	Provide immediate communication to response personnel.
	Security measures:	Rapid, dependable diverse means of communication such as phones, cell phones, pagers, radio links.
5.	Security objective:	Provide a means to detect loss through verification.
	Security measures:	Daily checking through physical checks, CCTV, 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 at least two layers of barriers (e.g. walls, cages) which together provide delay sufficient to enable response personnel to interdict.

Response

1.	Security objective:	Respond to assessed alarm in time and with sufficient resources to interrupt and prevent the unauthorised removal.
	Security measures:	Capability for timely response with size, equipment and training to interdict.

Security Management

1.	Security objective:	Provide access controls to source location that permits access to authorised persons only.
	Security measures:	Identification and verification, e.g. lock controlled by swipe card reader and personal identification number (PIN), 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.

APPENDIX-IX

GUIDELINES TO PREPARE SECURITY PLAN FOR INDUSTRIAL GAMMA RADIOGRAPHY/HDR BRACHYTHERAPY FACILITY (SOURCE CATEGORY 2 AND SECURITY LEVEL-B)

The security plan should be prepared addressing the issues in **Appendix VII**. 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.

APPENDIX-X

GUIDELINES TO PREPARE SECURITY PLAN FOR FACILITY HANDLING WELL LOGGING SOURCES/FIXED NUCLEONIC GAUGES (SOURCE CATEGORY 3 AND SECURITY LEVEL-C)

The security plan should be prepared addressing the issues in **Appendix-VII**. 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.

Detect

1.	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
2.	Security objective:	Provide immediate assessment of detection
	Security measures:	Assessment by operator / response personnel
3.	Security objective:	Provide a means to detect loss through verification
	Security measures:	Monthly checking through physical checks, tamper indicating devices, etc.

Delay

1.	Security objective:	Impede the unauthorised removal
	Security measures:	One barrier (e.g. cage, source housing) or observation by operating personnel

Response

1.	Security objective:	Implement appropriate action in the event of unauthorised removal of source
	Security measures:	Procedures for identifying necessary action in accordance with contingency plans

Security Management

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

	Security measures:	One identification measure
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 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 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

APPENDIX-XI

GUIDELINES TO PREPARE SECURITY PLAN FOR FACILITY HANDLING PORTABLE GAUGES/ TECHNETIUM GENERATORS (SOURCE CATEGORY 4 AND SECURITY LEVEL-D)

The security plan should be prepared addressing the issues in **Appendix-VII**. The security plan should also indicate the prudent measure(s) in place to ensure security of assets and their periodic verification. Given below are the security objectives against each of which, some security measures have been suggested.

The natural interest of the owner to protect the asset and to ensure safe use and storage is the appropriate basis for the security provided.

Security Management:

1.	Security objective:	Ensure safe use of the source and adequately protect it as an asset
	Security measures:	Apply the relevant safety standards as well as appropriate industrial standards. Verify the presence of the source at set intervals
2.	Security objective:	Ensure reliability of personnel
	Security measures:	The personnel in-charge of managing sources of Level D should be approved as legitimate authorised personnel

BIBLIOGRAPHY

1. The Industrial Radiography (Radiation Surveillance) Procedures, 1980.
2. Radiation Protection Rules, 1971.
3. Atomic Energy (Radiation Protection) Rules, 2004.
4. FOOD AND AGRICULTURE ORGANISATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANISATION, NUCLEAR ENERGY AGENCY OF THE ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, PAN AMERICAN HEALTH ORGANISATION, WORLD HEALTH ORGANISATION, International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources, Safety Series No. 115, IAEA, Vienna (1996).
5. INTERNATIONAL ATOMIC ENERGY AGENCY, Code of Conduct on the Safety and Security of Radioactive Sources, IAEA, Vienna (2004).
6. INTERNATIONAL ATOMIC ENERGY AGENCY, Categorisation of Radioactive Sources, Safety Guide No. RS-G-1.9, IAEA, Vienna (2005).
7. ATOMIC ENERGY REGULATORY BOARD, Security of Radioactive Material during Transport, Safety Guide No. AERB/NRF-TS/SG-10, Mumbai, India (2008).
8. INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Sources, Nuclear Security Series No. 11, IAEA,Vienna (2009).

LIST OF PARTICIPANTS

COMMITTEE TO DEVELOP GUIDE ON SECURITY OF RADIOACTIVE SOURCES IN RADIATION FACILITIES (CDGSRS)

Dates of meeting	:	January 19, 2007 February 14, 2007 March 22, 2007 April 17, 2007 May 1, 2007 June 14, 2007

Members and Invitees of CDGSRS:

Dr. A.N. Nandakumar (Convenor)	:	AERB (Former)
Shri S.P. Agarwal	:	AERB (Former)
Shri T.K. Jayakumar	:	BRIT (Former)
Dr. Pradeep Kumar	:	BARC
Shri R. Kannan	:	AERB (Former)
Dr. P.K. Dash Sharma	:	AERB
Dr. A.U. Sonawane (Member Secretary)	:	AERB
Shri K. Muralidhar (Invitee)	:	DAE (Former)
Shri Pravin J. Patil (Invitee)	:	AERB

ADVISORY COMMITTEE ON RADIOLOGICAL SAETY (ACRS)

Dates of meeting	:	October 11, 2007

Members and Invitees of ACRS:

Dr. U.C. Mishra (Chairman)	:	BARC (Former)
Dr. A.R. Reddy (Vice-Chairman)	:	DRDO, New Delhi (Former)
Dr. Gurusharan Singh	:	BARC
Dr. B.C. Bhatt	:	BARC (Former)
Dr. S.K. Shrivastava	:	Tata Memorial Hospital, Mumbai
Dr. (Smt.) Meera Venkatesh	:	BARC
Shri S.P. Agarwal (Member Secretary)	:	AERB (Former)

ADVISORY COMMITTEE ON SECURITY (ACS)

Date of meeting	:	September 7, 2007 October 11, 2007 November 2, 2007 June 9, 2010 August 11, 2010

Members and Invitees of ACS:

Shri G.P. Srivastava (Chairman)	:	BARC
Shri T.P. Das	:	DAE
Dr. A.K. Kohli	:	BRIT
Shri G. Nageswara Rao	:	NPCIL
Shri W.S. Aruldossa Kanthiah	:	HWB
Dr. P. Swaminathan	:	IGCAR
Shri R.I. Gujarathi	:	AERB
Shri R. Venkataraman	:	AERB (Former)
Shri S.N. Rao	:	AERB
Shri S.P. Agarwal	:	AERB (Former)
Shri S.A. Hussain	:	AERB
Shri R. Bhattacharya	:	AERB
Shri Fredric Lall (Member Secretary)	:	AERB
Shri S. Bhattacharya (Co-opted Member)	:	BARC
Shri L.B. Mahale (Permanent Invitee)	:	AERB
Shri S.K. Pradhan (Parmanent Invitee)	:	AERB

PROVISIONAL LIST OF REGULATORY DOCUMENTS ON SECURITY OF RADIOACTIVE MATERIALS/SOURCES

Safety Series No.	Titles
AERB/RF-RS/SG-1	Security of Radioactive Sources in Radiation Facilities
AERB/NRF-TS/SG-10	Security of Radioactive Material During Transport

AERB SAFETY GUIDE NO. AERB/RF-RS/SG-1

Published by **:** Atomic Energy Regulatory Board
Niyamak Bhavan, Anushaktinagar
Mumbai - 400 094
INDIA.

BCS