Australian Government

Australian Radiation Protection and Nuclear Safety Agency

arpansa

# Code of Practice for the Security of Radioactive Sources

## Radiation Protection Series No. 11

# Radiation Protection Series

The Australian Radiation Protection and Nuclear Safety Agency (ARPANSA) publishes Fundamentals, Codes and Guides in the Radiation Protection Series (RPS), which promote national policies and practices that protect human health and the environment from harmful effects of radiation. ARPANSA develops these publications jointly with state and territory regulators through the Radiation Health Committee (RHC), which oversees the preparation of draft policies and standards with the view of their uniform implementation in all Australian jurisdictions. Following agreement and, as relevant, approvals at the Ministerial level, the RHC recommends publication to the Radiation Health and Safety Advisory Council, which endorses documents and recommends their publication by the CEO of ARPANSA.

To the extent possible and relevant for Australian circumstances, the RPS publications give effect in Australia to international standards and guidance. The sources of such standards and guidance are varied and include the International Commission on Radiological Protection (ICRP); the International Commission on Non-Ionizing Radiation Protection (ICNIRP); the International Atomic Energy Agency (IAEA); and the World Health Organization (WHO).

***Fundamentals*** set the fundamental principles for radiation protection and describe the fundamental radiation protection, safety and security objectives. They are written in an explanatory and non-regulatory style and describe the basic concepts and objectives of international best practice.

***Codes*** are regulatory in style and may be referenced by regulations or conditions of licence. They contain either general safety or security requirements which may be applicable for all dealings with radiation, or practice-specific requirements. They provide overarching requirements and are expressed as 'must' statements which are to be satisfied to ensure an acceptable level of safety and/or security.

***Guides*** provide recommendations and guidance on how to comply with the Codes or apply the principles of the Fundamentals. They are written in an explanatory and non-regulatory style and indicate the measures recommended to provide good practice. They are generally expressed as 'should' statements.

These three categories of publications are informed by public comment during drafting and are subject to a process of assessment of regulatory impact.

All ARPANSA publications (including earlier editions of codes and guides for which ARPANSA is now responsible) are available in electronic format, and can be downloaded free of charge by visiting ARPANSA's website at https://www.arpansa.gov.au/regulation-and-licensing/regulatory-publications/radiation-protection-series.

Further information can be obtained by telephoning ARPANSA on 1800 022 333 (free call within Australia) or +61 (03) 9433 2211.

Australian Government
Australian Radiation Protection and Nuclear Safety Agency

arpansa

# Code of Practice for the Security of Radioactive Sources

## *Radiation Protection Series No. 11*

## January 2019

This publication was approved by the Radiation Health Committee on 28 November 2006 and on 8 December 2006 the Radiation Health and Safety Advisory Council advised the CEO to adopt the Code of Practice

The amendment to this publication (reflecting current nomenclature and publications) was approved by the Radiation Health Committee on 7 June 2017

© Commonwealth of Australia 2019

This publication is protected by copyright. Copyright (and any other intellectual property rights, if any) in this publication is owned by the Commonwealth of Australia as represented by the Australian Radiation Protection and Nuclear Safety Agency (ARPANSA).

ISBN 978-0-6483704-0-6
ISSN 1445-9760

**Creative Commons**

With the exception of the Commonwealth Coat of Arms, any ARPANSA logos and any content that is marked as being third party material, this publication, *Security of Radioactive Sources (2019)*, by the Australian Radiation Protection and Nuclear Safety Agency is licensed under a Creative Commons Attribution 3.0 Australia licence (to view a copy of the licence, visit *http://creativecommons.org/licenses/by/3.0/au*). It is a further condition of the licence that any numerical data referred to in this publication may not be changed. To the extent that copyright subsists in a third party, permission will be required from the third party to reuse the material.

In essence, you are free to copy, communicate and adapt the material as long as you attribute the work to ARPANSA and abide by the other licence terms. The works are to be attributed to the Commonwealth as follows:-

"© Commonwealth of Australia 2019, as represented by the Australian Radiation Protection and Nuclear Safety Agency (ARPANSA)"

The publication should be attributed as: Security of Radioactive Sources (2019).

**Use of the Coat of Arms**

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.dpmc.gov.au/government/commonwealth-coat-arms).

Enquiries regarding the licence and any use of this report are welcome.

ARPANSA
619 Lower Plenty Road
YALLAMBIE VIC 3085
Tel: 1800 022 333 (Freecall) or +61 3 9433 2211

Email: info@arpansa.gov.au
Website: www.arpansa.gov.au

The mission of ARPANSA is to protect people and the environment from the harmful effects of radiation.

Published by the Chief Executive Officer of ARPANSA in January 2007. Amendment published in January 2019.

## Acknowledgement of Country

ARPANSA proudly acknowledges Australia's Aboriginal and Torres Strait Islander community and their rich culture and pays respect to their Elders past and present. We acknowledge Aboriginal and Torres Strait Islander people as Australia's first peoples and as the Traditional Owners and custodians of the land and water on which we rely.

We recognise and value the ongoing contribution of Aboriginal and Torres Strait Islander people and communities to Australian life and how this enriches us. We embrace the spirit of reconciliation, working towards the equality of outcomes and ensuring an equal voice.

# Foreword

In 2002, the Radiation Health Committee (RHC) considered the security of Australia's sealed radioactive sources in the light of the increased potential for such sources to be used in terrorism. Later in the same year, the Committee published a national strategy and action plan which included a recommendation that a national set of security requirements be developed for sealed radioactive sources. This Code gives effect to the recommendation.

The Code has been developed on the basis that security outcomes should apply in a graded manner, that is, the stringency of the security measures should be proportional to the likelihood of the source or aggregation of sources being acquired and the consequences of malicious use. Using a risk management methodology that draws on the International Atomic Energy Agency's (IAEA) *Categorization of Radioactive Sources Safety Guide*, IAEA Safety Standard Series No. RS-G.1.9[1], the Code of Practice categorises radioactive sources into five categories and allocates security outcomes commensurate with the risk posed by sources in each category. In practice, the Code only requires additional security measures, other than reporting of security breaches, for Category 1, 2 and 3 sources because the security measures in place for safety purposes are considered adequate to ensure the physical security of Category 4 and 5 sources.

While the Code of Practice sets clear objectives for improving the security of radioactive sources, its effective implementation relies on the development and maintenance of an effective security culture. Such a culture consists of characteristics and attitudes in organisations, and of individuals, that ensure security issues receive the attention warranted by their significance. It is vital that this culture be instilled as early as possible.

**John Loy PSM**
**CEO of ARPANSA**

23 January 2007

[1] This document is available on the internet at web address: http://www-pub.iaea.org/MTCD/publications/PDF/Pub1227_web.pdf

(This page intentionally left blank)

# Contents

(This page intentionally left blank)

# 1. Introduction

The *Code of Practice for the Security of Radioactive Sources* gives effect to the agreement of the Radiation Health Committee in November 2002, that a set of security outcomes be developed and considered for inclusion in the *National Directory for Radiation Protection*.

## 1.1 Purpose

The purpose of this Code of Practice is to set out the security requirements to be implemented by persons dealing with a radioactive source in order to decrease the likelihood of the unauthorised access to or acquisition of the radioactive source by persons with malicious intent.

It is intended that this Code be given the force of law by each State and Territory and the Commonwealth, and administered by the regulatory authority in each jurisdiction as part of the regulatory framework governing the use of radiation.

## 1.2 Scope

This Code of Practice applies to a person dealing with a sealed radioactive source other than in circumstances where the *Civil Aviation Act 1988* or the *Navigation Act 1912* apply to that person.

This Code does not apply to a person dealing with an unsealed radioactive source.

## 1.3 Application of this code of practice

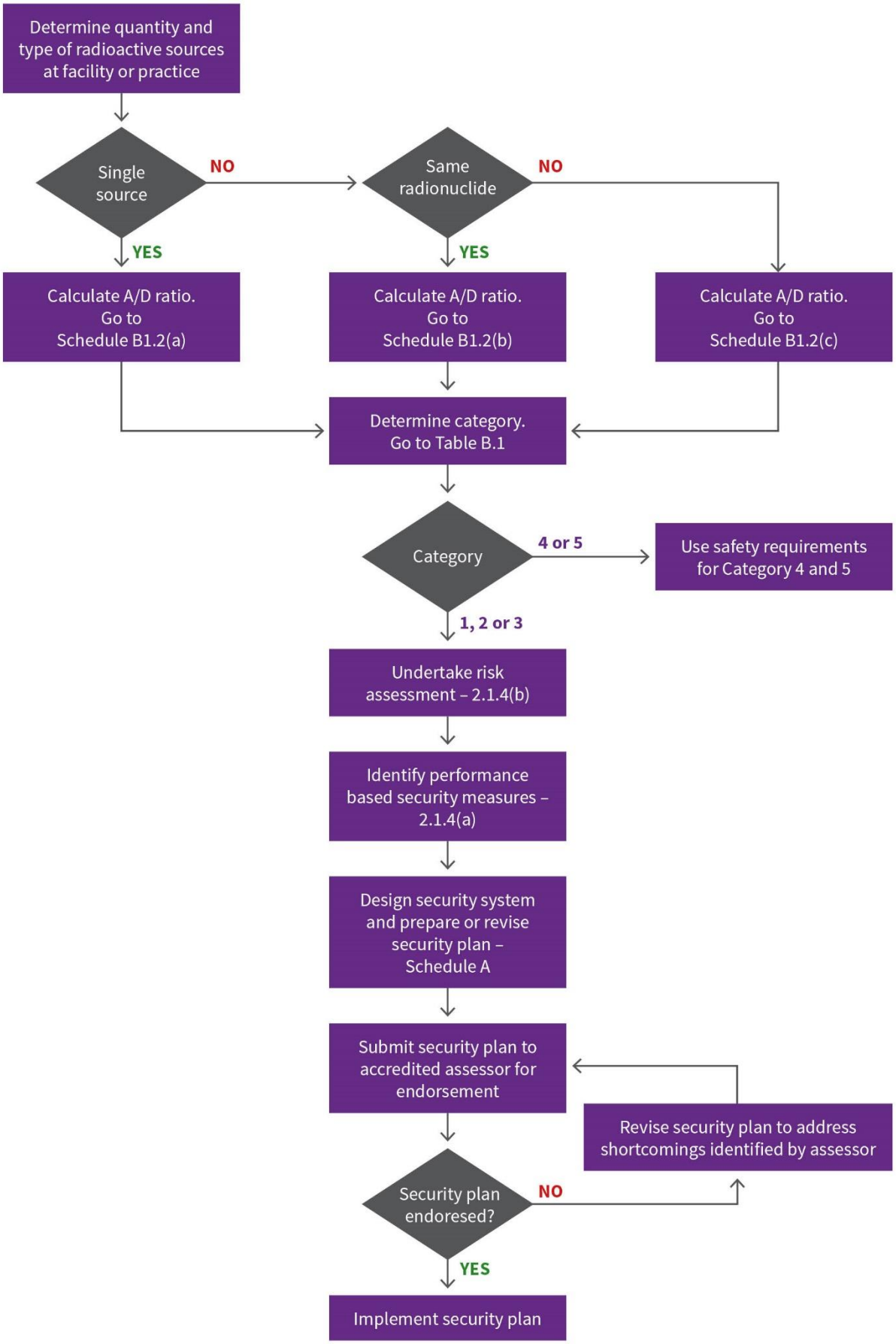
The security requirements to be applied to a radioactive source depend on the category of the radioactive source and the threat level for a radiological attack set by the Australian Government. In accordance with the National Counter Terrorism Plan[2], the threat level and accompanying threat assessment will be communicated to state and territory police. The police will then communicate information about the threat and the threat level to the regulatory authority or to the person responsible for managing the source (referred to in this Code as the Responsible Person), consistent with the National Counter Terrorism Handbook. Further information about the threat levels can be found in Schedule C.

This Code of Practice categorises radioactive sources into five categories and allocates security outcomes commensurate with the risk posed by sources in each category. This categorisation was informed by risk analyses that considered the major applications of radioactive material in Australia. Category 1 sources are considered to pose the highest risk and are therefore subject to the most stringent security outcomes. In practice, the Code only requires additional security measures, other than reporting of security breaches, for Category 1, 2 and 3 sources because the security measures in place for safety purposes are considered adequate to ensure the physical security of Category 4 and 5 sources. Each Category 1, 2 and 3 source will be subject to a security plan that must be endorsed by an assessor accredited by the regulatory authority.

The threat levels grade from ‘not expected ’ to ‘certain’. The Code links expected procedural and administrative security requirements to the threat level. A change in the threat level would change the procedural and administrative security requirements a person dealing with a Category 1, 2 or 3 radioactive source must perform. Figure 1 is a logic flow chart representation for the application of the Code.

[2] Available from http://www.nationalsecurity.gov.au/agd/www/nationalsecurity.nsf/Page/Publications

**Figure 1 – logic flowchart for source security**



While the Code of Practice sets clear objectives for improving the security of radioactive sources, its effective implementation relies on the development and maintenance of an effective security culture. Such a culture consists of characteristics and attitudes in organisations, and of individuals, that ensure security issues receive the attention warranted by their significance. It is vital that this culture be instilled as early as possible.

## 1.4 Related information

Additional guidance documents addressing the application of the Code (for both users and regulators) will be developed in consultation with the Radiation Health Committee.

Further information on the measures for improving security may be obtained from the current edition of the Attorney General's Department's Commonwealth Protective Security Policy Framework.

Guidance on equipment endorsed by the Attorney General's Department's Security Construction and Equipment Committee (SCEC) for use in security applications may be obtained from the current edition of the *Security Equipment Catalogue*, available via the Australian Security and Intelligence Organisation (ASIO) website at www.asio.gov.au.

Further information regarding risk-management principles and their practical implementation can be found in the international standard ISO 3100 and the associated Principles and Guidelines.

# 2. Source security – responsibilities and duties

## 2.1 Responsibilities of responsible person

### Source categorisation

2.1.1 Each Responsible Person dealing with a radioactive source must ensure that each radioactive source or aggregation of radioactive sources under that person's control is assigned a security category based on the methodology specified in Schedule B.

### Category 4 and 5 source

2.1.2 The Responsible Person dealing with a radioactive source or aggregation of radioactive sources assessed as being in categories 4 or 5 must comply with Chapter 7 of the Code.

### Category 1, 2 and 3 source – source security plan

2.1.3 The Responsible Person dealing with a security enhanced source other than for the purposes of transporting the source must:

(a) formulate a Source Security Plan that demonstrates how the Responsible Person will satisfy the requirements of this Code in relation to the source and includes the information described in paragraph A.1 of Schedule A

(b) have the Source Security Plan formulated in 2.1.3(a) endorsed by an assessor accredited for this purpose by the regulatory authority

(c) ensure that the Source Security Plan is implemented and complied with

(d) in the event that there is a change in the environment in which the dealing occurs - including new credible threat information - such that the Source Security Plan is no longer current, the Responsible Person must:

i. submit, for endorsement in accordance with 2.1.3(b), a revised Source Security Plan addressing the change

ii. implement and comply with the revised Source Security Plan.

### Security enhanced source – security requirements

2.1.4 For each security enhanced source the Responsible Person must ensure that the source is protected by measures that:

(a) meet the security outcomes specified in Chapters 3, 4, 5 and 6 of this Code as they apply to the relevant category of the source

(b) have been developed using a risk-based process that:

i. describes the source, the nature of the dealing, the environment in which the dealing occurs and existing security measures that protect the source

ii. identifies the credible threats to the source in relation to the dealing and the likelihood and consequence of the threats occurring

iii. initially, and during review processes, assesses the effectiveness of existing security measures to achieve the security outcomes taking into account the threat

iv. if required, identifies further or amended security measures necessary to achieve the security outcome.

## Security enhanced source - access

2.1.5 A Responsible Person who is a natural person or, if the Responsible Person is not a natural person, the natural person who oversees the implementation of the Code and associated security plans on behalf of the Responsible Person, must not deal with a security enhanced source unless the person has undergone a security background check in accordance with the requirements specified in Schedule E2.

2.1.6 The Responsible Person must ensure that a natural person (the 'second person') does not transport a security enhanced source unless the second person has a legitimate reason for transporting the source and has undergone a security background check in accordance with the requirements specified in Schedule E2.

2.1.7 Notwithstanding the transport measures in 2.1.6, the Responsible Person must ensure that a natural person, (the 'second person') does not deal with a security enhanced source unless the second person has a legitimate reason for dealing with the source and:

(a) for fixed or mobile sources:

i. has undergone an identity check in accordance with the requirements specified in Schedule E1
or

ii. is accompanied at all times by a person who satisfies the requirements of 2.1.7(a)(i)

(b) for portable sources:

i. has undergone a security background check in accordance with the requirements specified in Schedule E2
or

ii. is accompanied at all times by a person who satisfies the requirements of 2.1.7(b)(i).

2.1.8 The Responsible Person must ensure that a natural person who is in the presence of a security enhanced source other than for the purposes of dealing with the source:

(a) for fixed or mobile sources, or portable sources in storage:

i. has undergone an identity check in accordance with the requirements specified in Schedule E1
or

ii. is accompanied at all times by a natural person who satisfies the requirements of 2.1.8(a)(i)
or

iii. is subject to rigorous personnel surveillance at all times.

(b) for portable sources which are not in storage:

i. has undergone a security background check in accordance with the requirements specified in Schedule E2
or

ii. is accompanied at all times by a natural person who satisfies the requirements of 2.1.8(b)(i).

### Compliance with code and source security plan

2.1.9 The Responsible Person dealing with a security enhanced source must comply with this Code and the Source Security Plan formulated in relation to that source under 2.1 and endorsed by an assessor accredited for this purpose by the regulatory authority.

### Awareness of threat level

2.1.10 The Responsible Person dealing with a security enhanced source must update the security arrangements for the source in accordance with the Source Security Plan when advised by the police or the regulatory authority of a change in the threat level for a radiological attack.

### Transfer and disposal of security enhanced source

2.1.11 The Responsible Person dealing with a security enhanced source must not transfer the ownership of the source without the prior written approval of the regulatory authority in the jurisdiction of origin.

2.1.12 The Responsible Person dealing with a security enhanced source must not dispose of the source without the prior written approval of the regulatory authority.

## 2.2 Responsibilities of service providers

2.2.1 Upon completion of a technical service, the Responsible Person must ensure that the security measures associated with a security enhanced source (that may have been temporarily disabled in order to perform the service) have been re-enabled or, if they are not able to be re-enabled, the Responsible Person must follow the course of action required by the Source Security Plan in the event that security features are not able to be re-enabled.

## 2.3 Responsibility of persons

2.3.1 The following conditions apply to all persons irrespective of their association to the Responsible Person.

2.3.2 A person, other than the Responsible Person, who deals with a security enhanced source, must comply with this Code and the Source Security Plan formulated in relation to that source under 2.1 and endorsed by an assessor accredited for this purpose by the regulatory authority.

2.3.3 A natural person, other than the Responsible Person, must not transport a security enhanced source unless the person has a legitimate reason for transporting the source and has undergone a security background check in accordance with the requirements specified in Schedule E2.

Responsibility for ensuring that the person has undergone a security background check is to be borne by the Responsible Person.

2.3.4 Notwithstanding the transport measures in 2.3.3, a natural person, other than the Responsible Person, must not deal with a security enhanced source unless the person has a legitimate reason for dealing with the source and:

(a) for fixed or mobile sources:

i. has undergone an identity check in accordance with the requirements specified in Schedule E1
or

ii. is accompanied at all times by a natural person who satisfies the requirements of 2.3.4(a)(i)

(b) for portable sources:

i. has undergone a security background check in accordance with the requirements specified in Schedule E2
or

ii. is accompanied at all times by a natural person who satisfies the requirements of 2.3.4(b)(i).

2.3.5 A natural person, other than the Responsible Person, must not be in the presence of a security enhanced source for purposes other than dealing with the source unless the person:

(a) for fixed or mobile sources, or portable sources in storage:

i. has undergone an identity check in accordance with the requirements specified in Schedule E1
or

ii. is accompanied at all times by a natural person who satisfies the requirements of 2.3.5(a)(i)
or

iii. is subject to rigorous personnel surveillance at all times.

(b) for portable sources which are not in storage:

i. has undergone a security background check in accordance with the requirements specified in Schedule E2
or

ii. is accompanied at all times by a natural person who satisfies the requirements of 2.3.5(b)(i).

2.3.6 A person must not interfere with, remove, alter, damage or render ineffective, any security measures provided to secure a radioactive source except for legitimate source removal, transport or technical service as covered in the Source Security Plan or Source Transport Security Plan.

2.3.7 A person must not abandon a radioactive source without lawful excuse.

2.3.8 When a Category 1 or 2 source is to be transferred between jurisdictions, the intended recipient must ensure that the regulatory authority in the jurisdiction in which the recipient resides has approved the transfer of the source.

# 3. Use of security enhanced source – physical security measures

## 3.1 Use of a security enhanced source

3.1.1 For the purposes of this Chapter, 'use' is taken to include:

(a) the manufacture, possession, installation, operation, maintenance, repair or disposal of a radioactive source but does not include transport or storage

(b) brief internals of time, as defined by the Source Security Plan, during breaks in the performance of any of the activities described in 3.3.1(a).

3.1.2 When in use, a Category 1 security enhanced source must be protected by, at a minimum, physical security measures capable of providing sufficient delay to allow immediate detection and assessment of the intrusion, and for a guard or police service to interrupt unauthorised removal of the source.

## 3.2 Security outcomes to be achieved by risk-based physical security measures

### Category 1 security enhanced source

3.2.1 When in use, a Category 1 security enhanced source must be protected by, at a minimum, physical security measures capable of providing sufficient delay to allow immediate detection and assessment of the intrusion, and for a guard or police service to interrupt unauthorised removal of the source.

### Category 2 security enhanced source

3.2.2 When in use, a fixed or mobile Category 2 security enhanced source must be protected by, at a minimum, physical security measures capable of providing sufficient delay to allow immediate detection and assessment of unauthorised access to the source.

### Category 3 security enhanced source

3.2.3 When in use, a fixed or mobile Category 3 security enhanced source must be protected by, at a minimum, physical security measures capable of preventing unauthorised access to the source by human force.

# 4. Storage of radioactive sources – physical security measures

## 4.1 Storage of a security enhanced source

4.1.1 For the purposes of this chapter, storage is taken to exclude brief intervals of time between periods of use (as the term is defined in Chapter 3).

## 4.2 Security outcomes to be achieved by risk-based physical security measures

### Category 1 security enhanced source

4.2.1 When being stored, a Category 1 security enhanced source must be protected by, at a minimum, physical security measures capable of providing sufficient delay to allow immediate detection and assessment of the intrusion, and for a guard or police service to interrupt unauthorised removal of the source.

### Category 2 security enhanced source

4.2.2 When being stored, a Category 2 security enhanced source must be protected by, at a minimum, physical security measures capable of providing sufficient delay to allow immediate detection and assessment of unauthorised access to the source location.

### Category 3 security enhanced source

4.2.3 When being stored, a Category 3 security enhanced source must be protected by, at a minimum, physical security measures capable of preventing unauthorised access to the source by human force.

# 5. Transport of radioactive sources – physical security measures

## 5.1 Source transport security plan

5.1.1 The Responsible Person transporting a Category 1, 2 or 3 security enhanced source must ensure that:

(a) a Source Transport Security Plan that demonstrates how the Responsible Person will satisfy the requirements of this Code in relation to the source and contains the information set out in paragraph A.2 of Schedule A is endorsed by an assessor accredited for this purpose by the regulatory authority of each jurisdiction in which the source will be transported

(b) where the Source Transport Security Plan specified in clause 5.1 relates to the shipment of:

i. a Category 1 security enhanced source, the endorsed plan is provided to the regulatory authority at least 7 calendar days in advance of the proposed date of shipment
or

ii. a Category 2 or 3 security enhanced source, the endorsed plan is provided to the regulatory authority, at least 7 calendar days in advance of the proposed date of the shipment or, if shipments are likely to occur on a frequent basis, the first occasion a shipment occurs

(c) in the event that there is a change in the environment provided for in the Source Transport Security Plan - including new credible threat information - such that the Source Security Plan is no longer current, the Responsible Person must:

i. submit a revised Source Transport Security Plan for approval in accordance with 5.1.1(a)

ii. provide the endorsed revised plan to the regulatory authority in accordance with 5.1.1(b).

## 5.2 Security outcomes to be achieved by risk-based physical security measures

### Category 1 security enhanced source

5.2.1 When being transported, a Category 1 security enhanced source must be protected by, at a minimum, physical security measures capable of providing sufficient delay to allow immediate detection and assessment of the intrusion, and for a guard or police service to interrupt unauthorised access to the source.

### Category 2 security enhanced source

5.2.2 When being transported, a Category 2 security enhanced source must be protected by, at a minimum, physical security measures capable of providing sufficient delay to allow immediate detection and assessment of unauthorised access to the source.

5.2.3 When being transported, a Category 3 security enhanced source must be protected by, at a minimum, physical security measures capable of preventing unauthorised access to the source by human force.

## 5.3 Compliance with code and source transport security plan

5.3.1 Prior to the shipment occurring, the Source Transport Security Plan formulated and submitted to the regulatory authority under 5.1 must be endorsed by an assessor accredited for this purpose by the regulatory authority.

5.3.2 The Responsible Person transporting a Category 1, 2 or 3 security enhanced source must comply with the Source Transport Security Plan formulated in relation to that source under 5.1 and endorsed by an assessor accredited for this purpose by the regulatory authority.

5.3.3 A person, other than the Responsible Person, transporting a Category 1, 2 or 3 security enhanced source must comply with the Source Transport Security Plan formulated in relation to that source under 5.1 and endorsed by an assessor accredited for this purpose by the regulatory authority.

# 6. Procedural security measures

## 6.1 Security outcomes to be achieved by risk-based procedural security measures

### Category 1 security enhanced source

6.1.1 When the threat level is not expected or possible, the Responsible Person must ensure that the Category 1 security enhanced source is protected by actions commensurate with the security outcomes achieved by the measures in row 2 column 2 of Table D.1.

6.1.2 When the threat level is probable, the Responsible Person must ensure that the Category 1 security enhanced source is protected by actions commensurate with the security outcomes achieved by the measures in row 2, column 3 of Table D.1.

6.1.3 When the threat level is expected or certain, the Responsible Person must ensure that the Category 1 security enhanced source is protected by actions commensurate with the security outcomes achieved by the measures in row 2, column 4 of Table D.1.

6.1.4 The Responsible Person must ensure that following an escalation of the threat level, the outcomes are able to be escalated to those corresponding to the next highest threat level within the time specified in the security plan and likewise thereafter.

### Category 2 security enhanced source

6.1.5 When the threat level is not expected or possible, the Responsible Person must ensure that the Category 2 security enhanced source is protected by actions commensurate with the security outcomes achieved by the measures in column row 3, column 2 of Table D.1.

6.1.6 When the threat level is probable, the Responsible Person must ensure that the Category 2 security enhanced source is protected by actions commensurate with the security outcomes achieved by the measures in row 3, column 3 of Table D.1.

6.1.7 When the threat level is expected or certain, the Responsible Person must ensure that the Category 2 security enhanced source is protected by actions commensurate with the security outcomes achieved by the measures in row 3, column 4 of Table D.1.

6.1.8 The Responsible Person must ensure that following an escalation of the threat level, the outcomes are able to be escalated to those corresponding to the next highest threat level within the time specified in the security plan and likewise thereafter.

### Category 3 security enhanced source

6.1.9 When the threat level is not expected or possible, the Responsible Person must ensure that the Category 3 security enhanced source is protected by actions commensurate with the security outcomes achieved by the measures in row 4, column 2 of Table D.1.

6.1.10 When the threat level is probable, the Responsible Person must ensure that the Category 3 security enhanced source is protected by actions commensurate with the security outcomes achieved by the measures in row 4, column 3 of Table D.1.

6.1.11 When the threat level is expected or certain, the Responsible Person must ensure that the Category 3 security enhanced source is protected by actions commensurate with the security outcomes achieved by the measures in row 4, column 4 of Table D.1.

6.1.12 The Responsible Person must ensure that following an escalation of the threat level, the outcomes are able to be escalated to those corresponding to the next highest threat level within the time specified in the security plan and likewise thereafter.

# 7. Security management

## 7.1 Notification of a security breach

7.1.1 In the event of a security breach, the Responsible Person dealing with a radioactive source must:

(a) in the event that the security breach is

i. detectable theft
ii. unexplained loss
iii. unauthorised damage
iv. unauthorised access
v. unauthorised transfer

notify:

i. the local police service and immediately thereafter,
ii. the regulatory authority

that a security breach has occurred and provide, as a minimum, the following information:

i. circumstances of the security breach
ii. steps taken or proposed to be taken to rectify the breach
iii. if a radioactive source is lost or stolen, any information that may assist in the recovery of the source

or

(b) in the event of any other security breach notify

i. the regulatory authority and immediately thereafter,
ii. the local police service

that a security breach has occurred and provide, as a minimum, the following information:

i. circumstances of the security breach
ii. steps taken or proposed to be taken to rectify the breach.

7.1.2 The Responsible Person must submit a written report of the incident containing the information described in 7.1.1 to the regulatory authority within 7 days of the date of the notification pursuant to 7.1.1.

7.1.3 Persons that deal with the radioactive source should be alert to suspicious behaviour in relation to not only the radioactive source and the asset in which it is housed but also the immediate environs. Such suspicious behaviour must be reported to the local police service and the regulatory authority.

## 7.2 Accountancy and records

7.2.1 Each Responsible Person dealing with a radioactive source must, at all times, be able to account for the whereabouts of that source.

7.2.2 The Responsible Person dealing with a security enhanced source, other than to perform a technical service involving a source located on the premises of another Responsible Person, must maintain records for that source that:

(a) detail the whereabouts, serial number or identification number of the radioactive source

(b) include a copy of the radioactive source certificate or other certification

(c) detail the physical and chemical composition of the isotope in the source

(d) detail the construction details and type of radioactive source

(e) detail the activity and date of measurement of the activity of the radioactive source

(f) detail the import, export, transfer, disposal or change in location (within or between premises controlled by the Responsible Person) of the radioactive source in the previous twelve months

(g) detail authorisations to deal with the radioactive source from the regulatory authority.

# Schedule A

## Security Plans

### A1 Source Security Plan

A1.1 A Source Security Plan for a security enhanced source must include:

(a) a description of the source including details such as isotope, activity and date of measurement, serial number and physical and chemical form

(b) a description of the radiation practice for which the source is used and the categorisation of the source calculated in accordance with the methodology set out in Schedule B

(c) a description of the specific location of the source in the building or facility where it is used or stored

(d) a plan of the building or facility in which the source is used or stored including the physical security measures used to protect the source and a definition of the secure area for the purposes of Schedule D

(e) allocation of responsibilities for security to competent and qualified persons with appropriate authority to carry out their responsibilities

(f) a description of the specific security concerns to be addressed, for example theft or sabotage, or mechanical or electronic failure of a physical security measure

(g) a description of the physical security measures that will be used to address the security concerns and meet the requirements of the Code

(h) a description of the procedural security measures that will be used to address the security concerns and meet the requirements of the Code including:

i. access control
ii. key control
iii. CCTV surveillance
iv. personal surveillance
v. identity checks and security background checks of personnel
vi. inventories and records related to the management of sources
vii. information security
viii. procedures to be followed before, during and after a technical service
ix. contingency and security response arrangements including notification of security breach
x. security education and awareness
xi. actions to be taken in the event of a change in threat level

(i) arrangements for review and revision of the Source Security Plan, including maximum time between reviews.

## A2 Source Transport Security Plan

A2.1 A Source Transport Security Plan for a security enhanced source must include:

(a) a description of the source to be transported including: isotope, activity (including date of measurement), physical and chemical form, serial number, transport packaging and the categorisation of the source calculated in accordance with the methodology set out in Schedule B

(b) a statement of the purpose or reason for which the source is being transported

(c) a description of the conveyance in which the source will be transported and the arrangements for securing the shipment during trans-shipment or other stops en route

(d) allocation of responsibilities for security to competent and qualified persons with appropriate authority to carry out their responsibilities

(e) the name, address and business and after hours contact details for the consignor, consignee, carrier and, where used, guard or police service

(f) a description of the specific security concerns to be addressed, for example theft or sabotage, or mechanical or electronic failure of a physical security measure

(g) a description of the physical security measures that will be used to address the security concerns and meet the requirements of the Code

(h) a description of the procedural security measures that will be used to address the security concerns and meet the requirements of the Code including:

i. arrangements for notifying, as deemed appropriate, local police service or the regulatory authority of each jurisdiction in which the source will be transported

ii. contingency or emergency procedures for vehicle accidents or breakdown and including, for Category 1 sources, a planned principal route and an alternative route

iii. security response arrangements including notification of security breach

iv. security briefing for persons involved in transporting the source including nature of the threat, threat level and contingency and security response arrangements

v. identity checks and security background checks of personnel

vi. information security

vii. means of communication between parties involved in transporting the source

viii. actions to be taken in the event of a change in threat level

(i) arrangements for review and revision of the Source Transport Security Plan, including maximum time between reviews.

# Schedule B

## Categorisation of a radioactive source or aggregation of radioactive sources

### B1 Categorisation of a radioactive source

B1.1 The Code has been developed on the basis that security requirements should apply in a graded manner, that is, the stringency of the security measures should be proportional to the risk of the source or aggregation of sources being acquired and the consequences of malicious use. Using a risk methodology that draws on the IAEA's Categorization of Radioactive Sources Safety Guide[3], IAEA Safety Standard Series No. RS-G-1.9, the Code categorised sources into 5 categories and sets security requirements for each category.

B1.2 In determining the appropriate category for a radioactive source, or aggregation of radioactive sources:

(a) The categorisation for a single radioactive source is to be assigned the value in column 1 of Table B.1, based on the calculated value of activity ratio in column 2 of Table B.1, where the relevant $D$ value for the radioactive source is determined from Table B.2

(b) Where there is an aggregation of radioactive sources of the same radionuclide, the aggregated ratio $\left(\frac{A}{D}\right)$ must be calculated by dividing the summed activities of the radionuclide by the appropriate $D$ value determined from Table B.2 using the equation:

$$\text{Aggregate}\left(\frac{A}{D}\right) = \sum_i \frac{Ai}{D}$$

The calculated ratio $\left(\frac{A}{D}\right)$ is then compared with the ratios $\left(\frac{A}{D}\right)$ given in Table B.1, thus allowing the set of sources to be categorised on the basis of activity.

(c) Where there is an aggregation of radioactive sources with various radionuclides, the aggregated ratio $\left(\frac{A}{D}\right)$ must be calculated separately for each radionuclide as detailed in B1.2 (b) above. Then the sum of the ratios A/D must be determined using the equation:

$$\text{Aggregate}\left(\frac{A}{D}\right) = \sum_i \left(\frac{A_{i,1}}{D_1}\right) + \sum_i \left(\frac{A_{i,2}}{D_2}\right) + \cdots + \sum_i \left(\frac{A_{i,n}}{D_n}\right)$$

Where $A_{i,n}$ = activity of each individual source $i$ of radionuclide $n$;

$D_n$ = $D$ value for radionuclide $n$.

(d) The aggregated ratio $\left(\frac{A}{D}\right)$ is then compared with the ratios $\left(\frac{A}{D}\right)$ given in Table B.1, thus allowing the set of sources to be categorised on the basis of the sum of the aggregated ratios $\left(\frac{A}{D}\right)$ for each radionuclide.

B1.3 Within any practice there may be a number of distinct sub-practices which a security enhanced source may be associated with from time to time. One example is storage versus use. These sub-practices must be considered separately for security purposes because the categorisation of sources when in storage might be different from that when they are in use. This means that the physical

[3] This document is available on the internet at web address:
http://www-pub.iaea.org/MTCD/publications/PDF/Pub1227_web.pdf

security requirements for sources in storage might be different from those required when they are in use.

**Table B.1 Categorisation of sources by activity ratio**

| Category | Activity radio (A/D)[a] |
|---|---|
| 1 | $\left(\frac{A}{D}\right) \geq 1000$ |
| 2 | $1000 > \left(\frac{A}{D}\right) \geq 10$ |
| 3 | $10 > \left(\frac{A}{D}\right) \geq 1$ |
| 4 | $1 > \left(\frac{A}{D}\right) \geq 0.01$ |
| 5 | $0.01 > \left(\frac{A}{D}\right) > \left(\frac{Exempt^{b}}{D}\right)$ |

(a) Where:

- A is the total activity of a specific radioactive source, or aggregation of radioactive sources, containing a particular radioactive isotope, in units of gigabecquerel (GBq)
- $D$ is the value specified in Column 2 of Table B.2, in units of GBq.

The $D$-value for the specific radionuclide corresponds to the activity level at which the radioactive source is considered to be a Dangerous Source. The ratio of the activity in the radioactive source to the corresponding $D$-value for the radionuclide in the source $\left(\frac{A}{D}\right)$, determines the category of the source.

(b) Exempt quantities are given in Schedule 4 of the National Directory for Radiation Protection.

**Table B.2 Activity for a dangerous source ($D$-value)[a]**

| Radionuclide | D-value Activity Level (GBq) |
|---|---|
| americium-241 | 60 |
| americium-241/beryllium | 60 |
| cadmium-109 | $2 \times 10^4$ |
| caesium-137 | 100 |
| californium-252 | 20 |
| cobalt-57 | 700 |
| cobalt-60 | 30 |
| curium-244 | 50 |
| gadolinium-153 | $1 \times 10^3$ |
| germanium-68 | 700 |
| gold-198 | 200 |
| iodine-125 | 200 |
| iodine-131 | 200 |
| iridium-192 | 80 |
| iron-55 | $8 \times 10^5$ |
| krypton-85 | $3 \times 10^4$ |
| molybdenum-99 | 300 |
| nickel-63 | $6 \times 10^4$ |
| palladium-103 | $9 \times 10^4$ |
| phosphorus-32 | $1 \times 10^4$ |
| plutonium-238 | 60 |
| plutonium-239/beryllium | 60 |
| polonium-210 | 60 |
| promethium-147 | $4 \times 10^4$ |
| radium-226 | 40 |
| ruthenium-106 (rhodium-106) | 300 |
| selenium-75 | 200 |
| strontium-90 (yttrium-90) | $1 \times 10^3$ |
| technetium-99m | 700 |
| thallium-204 | $2 \times 10^4$ |
| thulium-170 | $2 \times 10^4$ |
| tritium (H-3) | $2 \times 10^6$ |
| ytterbium-169 | 300 |

(a) If an isotope is not mentioned in this table, contact the regulatory authority for the relevant $D$ value.

# Schedule C

## Threat level

### C1 Description

C1.1 The threat level is an indicator of the likelihood of a perceived perpetrator to acquire radioactive sources for the purposes of malicious use in Australia. Threat levels are set by the Australian Government's National Threat Assessment Centre in relation to specific people, places, events, sectors and interests. Local threat levels may also be informed by intelligence gathered at the State and Territory level. Responsible Persons will be informed of an escalation subject to jurisdictional arrangements. Procedural security measures for protecting a security enhanced source escalate in accordance with the threat level.

C1.2 The threat levels are as specified in Table C.1.

**Table C.1. Threat levels**

| Threat Levels |
|---|
| Certain |
| Expected |
| Probable |
| Possible |
| Not expected |

# Schedule D

## Procedural and administrative security requirements

**Table D.1 Scalability of procedural and administrative security requirements with threat level for a security enhanced source**

| Source category | Threat Level | | | |
|---|---|---|---|---|
| | Not expected or possible | Probable | Expected or certain | Row 1 |
| **1** | A, D | A, B, D, E | A, B, C, D, E | Row 2 |
| **2** | A | A, B, D, E | A, B, C, D, E | Row 3 |
| **3** | A | A, B | A, B, C, D, E | Row 4 |
| Column 1 | Column 2 | Column 3 | Column 4 | |

**Legend**

| Group | Security action |
|---|---|
| **A** | Annual review of Source Security Plan and Source Security Transport Plan |
| | Annual review of intrusion detection, event assessment and communication measures |
| | Annual review of access controls and physical barriers |
| | Annual review of staff access requirements |
| | Event specific review of staff access |
| | Staff induction security awareness briefing |
| | Annual staff security awareness briefing |
| | Event specific staff security awareness briefing |
| | Annual audit of all sources |
| | Monthly accounting or check to confirm present of the source |
| | Visitors to be signed in and escorted while present inside the secure area defined in the Source Security Plan |
| **B** | Weekly accounting or check to confirm presence of the source |
| **C** | Visitors to be refused entry to the inside of the secure area defined in the Source Security Plan, unless authorised by the regulatory authority police |
| | Goods deliveries to be dispatched and received off-site with movement of goods only to be undertaken by personnel satisfying 2.1.8 or 2.1.9 |
| | Half yearly staff security awareness briefing |
| | Daily accounting or check to confirm presence of the source |
| **D** | Annual exercising of guard force or police service response arrangements |
| **E** | Half yearly review of staff access |

# Schedule E

## Identity check and security background check

### E1 Procedures for performing an identity check

E1.1 The identity of each person who is intended to have access to a security enhanced source must be verified by:

(a) provision of original identity documents in accordance with E1.2

(b) confirmation of employment history, education and personal referees

(c) to the extent necessary, obtaining independent information to corroborate that provided by the person, for example, seek references not supplied by the person.

E1.2 Each person who has access to a security enhanced source must provide one original document from Table E.1 and one original document from Table E.2.

**Table E.1 Primary identity document**

| |
|---|
| Australian full birth Certificate showing parental details |
| An overseas birth certificate showing parental details provided a passport or an official Australian Travel document is also shown. |
| A current Document of Identity issued by the Australian Passport Office. |
| A current Australian passport or one that expired within the last two years. |
| A current foreign passport. |
| An Australian naturalisation or citizenship document or immigration papers issued by the Commonwealth Department of Immigration and Multicultural and Indigenous Affairs. |
| A current driver's licence from an Australian State or Territory or one that expired within the last two years. |

**Table E.2 Secondary identity document**

| |
|---|
| A current Medicare card, Pensioner Concession Card, Department of Veterans' Affairs entitlement card or any other current entitlement card issued by the Commonwealth Government. |
| A current credit card that shows the person's name, or account card from a bank, building society or credit union, or a passbook or account statement up to one year old. |
| An armed services discharge document up to two years old. |
| A current student identity card or a certificate or statement of enrolment up to two years old from an educational institution. |
| An electoral enrolment card or other evidence of enrolment not more than two years old. |
| A telephone, gas or electricity bill up to one year old. |
| A water rates, council rates or land valuation notice up to two years old. |

## E2 Security background check

E2.1 In addition to the identity check detailed in E1, the person must have a security background check. The security background check includes a security assessment in respect of a person, issued by ASIO, and criminal history checks by the Australian Federal Police, and all State and Territory police services.

# Glossary

**Activity**
the measure of quantity of radioactive materials, except when used in the term 'human activity'.

Activity, *A*, is a measure of the amount of a radioactive material given by:

$$A = \frac{dN}{dt}$$

where $dN$ is the expectation value of the number of spontaneous nuclear transitions which take place in the time interval $dt$.

The unit of activity is $s^{-1}$ with the special name becquerel (Bq).

**Aggregation of radioactive sources**
radioactive sources are considered to be aggregated if breaching a common physical security barrier (e.g., a locked door at the entrance to a storage room) would allow access to the sources or devices containing the sources.

**Code**
the Code of Practice for the Security of Radioactive Sources.

**Code of Practice for the Security of Radioactive Sources**
the document of that title published by the CEO of the Australian Radiation Protection and Nuclear Safety Agency in 2006.

**Deal with**
includes to use, manufacture, store, sell, receive, possess, install, operate, maintain, repair, dispose of or transport a radioactive source.

**Dealing**
includes to use, manufacture, store, sell, receive, possess, install, operate, maintain, repair, dispose of or transport a radioactive source.

**Fixed radioactive source**
a radioactive source located in a device or container which, in the normal course of its use, is permanently secured to a structure and intended to be immobile.

**Human force**
any force that can be exerted by a natural person including by using tools, but excluding the use of power tools.

**Mobile radioactive source**
a radioactive source located in a device or container which, in its normal course of use, is intended to be capable of being moved in a limited way from place to place, for example a large machine on wheels designed to be able to be repositioned by a person within a room in a facility.

**Physical security measure**
a tangible barrier intended to deter and delay unauthorised access to a radioactive source.

**Portable radioactive source**
a radioactive source located in a device or container which, in its normal course of use, is intended to be carried or moved with ease from place to place.

**Radioactive source**
a sealed radioactive source.

**Radioactive material**
material that undergoes spontaneous transformation of its nucleus with the emission of ionizing radiation and which, for the purposes of this Code, exceeds a prescribed concentration or activity as determined by the relevant regulatory authority.

**Regulatory authority**
an entity or organisation or a system of entities or organisations designated by the government of a State, Territory or the Commonwealth as having legal authority for exercising regulatory control with respect to radioactive sources, including issuing authorisations, and thereby regulating one or more aspects of the safety or security of radioactive sources.

**Responsible person**
a natural person or a body corporate who deals with a sealed radioactive source and either:

(a) has the direct management responsibility for the security of the source or the premises; or

(b) has the overall control over who may use the source or premises.

**Rigorous personnel surveillance**
recorded surveillance by:

(a) a monitored closed circuit television (CCTV) camera; or

(b) an event actuated camera; and

(c) anti stay behind detection and alarm.

**Routine maintenance**
work intended by the manufacturer of the radioactive source or equipment housing the source to be performed by the Responsible Person in order to keep the source or equipment in adequate operating order.

**Sealed radioactive source**
radioactive material that is permanently sealed in a capsule or closely bonded in a solid form.

**Secure**
free from:

(a) detectable theft

(b) unexplained loss

(c) unauthorised damage

(d) unauthorised access

(e) unauthorised transfer.

**Security**
measures to prevent unauthorised access or damage to, and loss, theft or unauthorised transfer of, a radioactive source.

**Security breach**
a breach of a security measure specified in the Source Security Plan or Source Transport Security Plan or the requirements of this Code.

**Security enhanced source**
a radioactive source or aggregation of radioactive sources assigned the Category 1, 2 or 3 when using the methodology set out in Schedule B.

**Security measure**
a stratagem or engineered device which is put in place as an element of a security system.

**Security plan**
a plan that has been put in place to effectively minimise all security risks relevant to the dealing with a Category 1, 2 or 3 radioactive source.

**Security risk**
risk of:

(a) theft of a radioactive source
(b) unexplained loss of a radioactive source
(c) unauthorised damage
(d) unauthorised access
(e) unauthorised transfer.

**Security system**
a combination of security measures described in a security plan which ensures the security of a security enhanced source.

**Service provider**
a person who is, or who employs, a service technician.

**Service technician**
a person, being a natural person, who repairs, performs maintenance, other than routine maintenance, or calibrates a radioactive source or a housing that contains a radioactive source.

**Technical service**
the performance of maintenance by a service technician, other than routine maintenance, on the equipment housing a security enhanced source or any other security measures in place to secure a security enhanced source.

**Unauthorised access**
in the context of this Code, means physical access gained to a security enhanced source without the lawful consent of a person entitled to grant such consent at law.

**Unexplained loss**
any documented loss that cannot be explained.

**Unsealed radioactive source**
a radioactive substance that is not a sealed radioactive source.