

# **Code of Practice for the Security of Radioactive Material**

ORS C5

Citation: Ministry of Health. 2020. *Code of Practice for the Security of Radioactive Material: ORS C5*. Wellington: Ministry of Health.

Published in April 2020 by the Ministry of Health  
PO Box 5013, Wellington 6140, New Zealand

ISBN 978-1-98-859784-3 (online)  
HP 7391



This document is available at [health.govt.nz](https://health.govt.nz)



This work is licensed under the Creative Commons Attribution 4.0 International licence. In essence, you are free to: share ie, copy and redistribute the material in any medium or format; adapt ie, remix, transform and build upon the material. You must give appropriate credit, provide a link to the licence and indicate if changes were made.

# Contents

<b>Introduction</b>	<b>1</b>
Purpose and commencement	1
Scope	1
Contact	1
<b>Key roles</b>	<b>2</b>
<b>Definitions</b>	<b>3</b>
<b>Security Management</b>	<b>6</b>
General	6
Use and storage	7
Transport	8
<b>Security system</b>	<b>10</b>
Unlawful removal	10
Missing or lost material	12
Sabotage	12
<b>Appendix 1: Assigning a security level for use and storage</b>	<b>13</b>
Secured area has no nuclear material	13
Secured area has only nuclear material	14
Secured area has both nuclear and non-nuclear material	15
<b>Appendix 2: Security level - transport</b>	<b>17</b>
Package contains no nuclear material	17
Package only contains nuclear material	18
Package contains both nuclear and non-nuclear material	18
<b>Appendix 3: D and A2-values</b>	<b>21</b>
<b>Appendix 4: Security goals</b>	<b>22</b>
<b>Appendix 5: Security plans</b>	<b>23</b>
<b>Appendix 6: Training</b>	<b>26</b>



# Introduction

## Purpose and commencement

This *Code of Practice for the Security of Radioactive Material: ORS C5* is issued by the Director for Radiation Safety under section 86 of the Radiation Safety Act 2016. It provides operational details on compliance with the security requirements in sections 11 and 12 of the Act, which relate to the security of radioactive material. The requirements in this code do not limit the general nature of the requirements in those sections of the Act.

This code of practice comes into force 12 months after the publication date.

## Scope

This code of practice applies to the security of radioactive material, facilities and associated activities for the prevention of malicious acts intended or likely to cause harmful radiological consequences.

Radioactive material includes sealed radioactive sources, unsealed radioactive sources, nuclear material and radioactive waste. The code applies throughout the lifetime of the radioactive material whether it is in use, storage or being transported.

The following are excluded from the scope of this code:

- safety and security requirements of irradiating apparatus used for medical diagnosis and therapy, industrial radiography, veterinary and other non-medical purposes
- safety of radioactive material used for medical diagnosis and therapy, industrial radiography, irradiation, veterinary and other non-medical purposes.

The above safety and security requirements are set out in the codes of practice specific to the type of radioactive material or what it is used for.

## Contact

Contact the Director for Radiation Safety:

Office of Radiation Safety  
PO Box 5013  
Wellington 6140

Email: [orsenquiries@health.govt.nz](mailto:orsenquiries@health.govt.nz)  
[health.govt.nz/our-work/ionising-radiation-safety](https://www.health.govt.nz/our-work/ionising-radiation-safety)

# Key roles

These individuals and bodies have roles and responsibilities in relation to this code of practice.

**Managing entity** – the legal entity that manages or controls radiation sources whether they are in use, storage or being transported. For material in use and storage, this is the person or organisation that must obtain a source licence as required by section 13(a) of the Act. For material being transported, this could be the consignor, carrier or consignee, depending on who is managing and controlling the material at the time and, therefore, has prime responsibility for its security. Where transport is a normal activity (such as industrial radiography and the use of nuclear density meters), the managing entity will usually be the same for use, storage and during transport.

**Office of Radiation Safety** – New Zealand’s regulatory body for the security of radioactive material.

**Radiation security officer** – a person who is designated by the managing entity to oversee the application of regulatory requirements for the security of radioactive material.

**Response personnel** – personnel such as officers of national organisations like New Zealand Police or New Zealand Defence Force who respond to a security event in order to interrupt or defeat an adversary.

# Definitions

Defined terms are in **bold**.

**A2 value** – the activity value of radioactive material other than **special form radioactive material** derived from the **IAEA Transport Regulations**, as set out in Appendix 3.

**Associated activity** – the possession, production, processing, use, storage, handling or disposal of radioactive material.

**Basic security package** – a package used to transport radioactive material that is not an **excepted security package** nor an **enhanced security package**. Security requirements for basic security packages are set out in clause 6 of this code.

**D value** – the activity level determined by the International Atomic Energy Agency used to categorise radioactive sources based on their potential to cause harm, as set out in Appendix 3.

**Defence in depth** – the combination of multiple layers of systems and measures that have to be overcome or circumvented before the security of radioactive material is compromised.

**Enhanced security package** – a package used to transport radioactive material that satisfies the applicable requirements in Appendix 2. Security requirements for enhanced security packages are set out in clause 7 of this code.

**Excepted security package** – a package used to transport radioactive material that satisfies the requirements for excepted packages in the **IAEA Transport Regulations**. Security requirements for excepted security packages are set out in clause 5 of this code.

**Facility** – the place where radioactive material is used or stored.

**High-activity radioactive material** – as defined in regulation 3 of the Radiation Safety Regulations 2016.

**IAEA Transport Regulations** – the latest edition of the *Regulations for the Safe Transport of Radioactive Material* issued by the International Atomic Energy Agency as No. SSR-6<sup>1</sup>.

**Insider** – an individual with authorised access to facilities, associated activities or to sensitive information or sensitive information assets, who could commit or facilitate the commission of a malicious act.

<sup>1</sup> Read the 2018 edition: [www-pub.iaea.org/MTCD/Publications/PDF/PUB1798\\_web.pdf](http://www-pub.iaea.org/MTCD/Publications/PDF/PUB1798_web.pdf)

**Low-activity radioactive material** – as defined in regulation 3 of the Radiation Safety Regulations 2016.

**Malicious act** – an act or attempt of unauthorised removal or sabotage of radioactive material.

**Nuclear material** – means any source material or any **special fissionable material**.

**Radioactive material** – material that spontaneously emits ionising radiation including sealed radioactive sources, unsealed radioactive sources, nuclear material and radioactive waste.

**Sabotage** – any deliberate act directed against a facility or an associated activity that could directly or indirectly endanger the health and safety of personnel, the public, or the environment by exposure to radiation or release of radioactive substances.

**Secured area** – an area with a single set of access controls in which radioactive material is used or stored.

**Security culture** – the assembly of characteristics, attitudes and behaviours of individuals, organisations and institutions that serves as a means to support, enhance and sustain the security of radioactive material.

**Security event** – an event including force majeure that has implications for the security of radioactive material.

**Security plan** – a written plan maintained by the managing entity that describes the security approach and system to protect the material. It complies with the requirements in Appendix 5.

**Sensitive information** – information, the unauthorised disclosure (or modification, alteration, destruction or denial of use) that could compromise the security of radioactive material or otherwise assist in carrying out a malicious act against a facility, organisation or transport. Sensitive information may refer to, for example, the security arrangements for radioactive material at a facility, the systems, structures and components at a facility, the location and details of transporting radioactive material, or details of an organisation's personnel.

**Source material** – (a) uranium containing a mixture of isotopes occurring in nature, uranium depleted in the isotope 235, or thorium; and (b) any material described in paragraph (a) that is in the form of metal, alloy, chemical compound, or concentrate; and (c) any material prescribed under regulations made on the recommendation of the Minister of Health with regard to any relevant determination made by the IAEA.

**Special fissionable material** – (a) plutonium-239, uranium-233, or uranium enriched in the isotopes 235 or 233 or both; or (b) any combination of the material described in paragraph (a); or (c) any material prescribed under regulations made on the recommendation of the Minister of Health with regard to any relevant determination made by the IAEA.



**Special form radioactive material** – a non-dispersible solid radioactive material or a sealed capsule containing radioactive material.

**Threat** – a person or group with motivation, intention or capability to commit a malicious act.

**Transport** – the deliberate physical movement of radioactive material from one place to another including in-transit storage that is incidental to that movement.

**Unacceptable radiological consequences** – an effective dose exceeding 100 mSv received by any member of the public in the first seven days following an event.

**Unauthorised access** – access or attempted access that is not inadvertent and has malicious intent.

**Unauthorised removal** – the theft or other unlawful taking of radioactive material.

**Vulnerability assessment** – evaluation and documentation of the features and effectiveness of the overall security system at a facility.

# Security Management

## General

1. The managing entity must:
  - (a) take prime responsibility for the security of radioactive material under its management or control
  - (b) assign a security level A, B, C or D to each:
    - (i) secured area in which radioactive material is to be used or stored, as set out in Appendix 1
    - (ii) package in which radioactive material is transported, as set out in Appendix 2
  - (c) establish a management system to enhance security that includes:
    - (i) effectively integrating security into the overall management system of the organisation
    - (ii) making a commitment to security from the highest level of management at the facility, and providing all required resources
    - (iii) promoting continuous improvement and a security culture
  - (d) for the use and storage of radioactive material in secured areas that are assigned security levels A, B or C and for transporting radioactive material in enhanced security packages:
    - (i) appoint a radiation security officer to oversee the application of regulatory requirements
    - (ii) ensure that, if they are different people, the radiation security officer and radiation safety officer work closely together so that radiation safety measures are not compromised
    - (iii) consult with and engage the services of experts and interested parties as necessary.
2. The managing entity must design and implement security requirements:
  - (a) in proportion to the potential consequences of a malicious act
  - (b) taking account of the current threat assessment
  - (c) in an integrated way by consulting qualified safety experts to ensure that radiation safety measures are not compromised by security requirements
  - (d) adopting the concept of defence in depth
  - (e) to ensure that:
    - (i) the security goals in Appendix 4 are met

- (ii) if there are two or more requirements in this code relating to the managing entity's activities then the more stringent of those requirements is applied
- (iii) there is a continuous chain of security when radioactive material is handed over from one party to another.<sup>2</sup>

## Use and storage

3. For using or storing radioactive material in secured areas that are assigned security levels A, B or C, the managing entity must:
  - (a) ensure that all staff and contractors with responsibilities for security:
    - (i) are qualified, educated and trained in security so that they understand their duties and can perform them competently
    - (ii) satisfy the training requirements, as set out in Appendix 6
    - (iii) are listed with details of their qualifications, education and training
    - (iv) are notified of their duties in relation to security
    - (v) are authorised to assume their roles and responsibilities
  - (b) conduct background checks to assess the trustworthiness and reliability of all persons with security responsibilities that include:
    - (i) confirming a person's identity with photo identification
    - (ii) verifying references
    - (iii) for security levels A and B, getting a Ministry of Justice criminal record check
    - (iv) for security level A, undertaking a five-yearly criminal record check
  - (c) restrict access to security-sensitive information by:
    - (i) identifying the information that must be protected
    - (ii) authorising the people who can access such information
    - (iii) preventing disclosure to unauthorised people
  - (d) establish processes for granting unescorted access to radioactive material or sensitive information to people who have demonstrated a need for such access
  - (e) provide access controls that verify a person's identity and authorisation to restrict unescorted access to areas where radioactive material is present for:
    - (i) security level A, by providing a combination of two or more verification measures (eg, a swipe card and a PIN; or the use of a

<sup>2</sup> Unless otherwise agreed, security responsibilities are transferred to another party when an individual with apparent authority accepts possession of the material on behalf of the receiving party.

- swipe card and a controlled key) that are protected against compromise such as manipulation or falsification
    - (ii) for security levels B and C, by at least one verification measure.
  - (f) provide and maintain a security plan that complies with the requirements set out in Appendix 5
  - (g) evaluate compliance and effectiveness, including performance testing
  - (h) establish the capability to manage and report security events.
4. For using or storing radioactive material in secured areas that are assigned security level D, the managing entity must secure the material:
- (i) in accordance with prudent management practice
  - (j) in a manner that impedes unauthorised removal of the material.

## Transport

5. For transporting radioactive material in excepted security packages, the managing entity must secure the package by:
- (a) securing and storing the package in a manner that impedes unauthorised removal
  - (b) not leaving packages or conveyances unattended for any longer than is necessary
  - (c) whenever possible:
    - (i) using carriers with package tracking systems
    - (ii) using closed vehicles to keep the packages out of sight.
6. For transporting radioactive material in basic security packages, the managing entity must:
- (a) meet the requirements in clause 5 for excepted security packages
  - (b) provide members involved in transporting with written details of emergency contacts
  - (c) check the backgrounds of authorised individuals to ensure that they are correctly identified, trustworthy and reliable
  - (d) provide basic security awareness training that includes:
    - (i) the need for transport security
    - (ii) the nature of security-related threats
    - (iii) methods to address security concerns and actions to take if there is a security event
  - (e) identify and protect sensitive information

- (f) provide adequate budget and resources
  - (g) evaluate compliance
  - (h) ensure capability to respond to security events
  - (i) establish capability for timely reporting of security events.
7. For transporting radioactive material in enhanced security packages, the managing entity must:
- (a) meet the requirements in clause 6 for basic security packages
  - (b) maintain a security plan that complies with the requirements set out in Appendix 5
  - (c) ensure the trustworthiness and reliability of authorised individuals
  - (d) ensure that staff members with responsibilities for security:
    - (i) are qualified, educated and trained in security so that they understand their duties and can perform them competently
    - (ii) satisfy the training requirements set out in Appendix 6
    - (iii) are listed with details of their qualifications, education and training
    - (iv) are notified of their duties in relation to security
    - (v) are authorised to assume their roles and responsibilities
  - (e) evaluate compliance and effectiveness including performance testing, exercises and drills
  - (f) ensure the capability to manage security events.

# Security system

## Unlawful removal

8. For radioactive material that is used or stored in secured areas that are assigned security level A, the managing entity must:
  - (a) verify and document the presence of each item of radioactive material daily
  - (b) provide measures to immediately detect any unauthorised access to the secured area
  - (c) provide measures to immediately detect any attempted unauthorised removal of radioactive material, including by an insider
  - (d) immediately assess and verify detections under clauses 8(b) and (c)
  - (e) provide delay after detection that:
    - (i) contains at least two layers of barriers, and
    - (ii) is sufficient for response personnel to interrupt the unauthorised removal of material
  - (f) provide a means to immediately communicate to response personnel
  - (g) provide for an immediate response with sufficient capability to interrupt and prevent the unauthorised removal
  - (h) upon verification of attempted unauthorised access or attempted or actual unauthorised removal under clause 8(d), immediately notify the Office of Radiation Safety incident officer (on 021 393 632) and New Zealand Police to follow their instructions
  
9. For radioactive material that is used or stored in secured areas that are assigned security level B, the managing entity must:
  - (a) verify and document the presence of each item of radioactive material:
    - (i) for portable devices, daily after use in the field
    - (ii) at least weekly in other cases
  - (b) provide measures to immediately detect any unauthorised access to the secured area<sup>3</sup>
  - (c) provide measures to detect any unauthorised removal of radioactive material

<sup>3</sup> For portable devices containing radioactive material when used in the field the requirements in clauses 9(b)-(d) normally require visual observation by 2 operator personnel

- (d) immediately assess and verify detections under clauses 9(b) and (c)
  - (e) provide delay after detection that have:
    - (i) at least two layers of barriers
    - (ii) means to affix portable devices containing radioactive material when used in the field to a stationary object
    - (iii) are sufficient for response personnel to interrupt the unauthorised removal of material
  - (f) provide a means to immediately communicate with response personnel
  - (g) provide for an immediate initiation of response to interrupt the unauthorised removal
  - (h) upon verification of attempted unauthorised access or attempted or actual unauthorised removal under clause 9(d), immediately notify the Office of Radiation Safety incident officer (on 021 393 632) and New Zealand Police to follow their instructions
10. For radioactive material that is used or stored in secured areas that are assigned security level C, the managing entity must:
- (a) verify and document the presence of each item of radioactive material at least monthly
  - (b) provide means to detect any unauthorised access to the secured area or unauthorised removal of radioactive material
  - (c) immediately assess and verify detections under clause 10(b)
  - (d) provide delay after detection that:
    - (i) have at least one barrier or the presence of operator personnel, and
    - (ii) is sufficient to provide confidence that the security system will prevent unauthorised removal of material
  - (e) provide a means to immediately communicate with response personnel
  - (f) upon verification of unauthorised removal under clause 10(c), immediately notify the Office of Radiation Safety incident officer (on 021 393 632) and New Zealand Police to follow their instructions
11. For radioactive material that is used or stored in secured areas that are assigned security level D, the managing entity must provide confidence that the security system will prevent unauthorised removal of the material.
12. For the transport of radioactive material in enhanced security packages, the managing entity must:
- (a) immediately detect any unauthorised access to the package
  - (b) detect any attempted unauthorised removal of the package
  - (c) immediately assess the detections under clauses 12(a) and (b)

- (d) verify package count and seal integrity upon delivery
  - (e) have delay measures in place to prevent unauthorised removal of packages
  - (f) provide a means to immediately communicate with response personnel
  - (g) immediately notify the Office of Radiation Safety incident officer (on 021 393 632) and New Zealand Police to follow their instructions
  - (h) immediately initiate a response to interrupt any unauthorised removal.
13. For transporting radioactive material in a basic security package, the managing entity must:
- (a) detect any unauthorised removal of the package
  - (b) verify the package count and seal integrity upon delivery
  - (c) notify any unlawful removal of the package to the Office of Radiation Safety.

## Missing or lost material

14. The managing entity must:
- (a) implement rapid and comprehensive measures to locate and recover missing or stolen material
  - (b) cooperate with and assist competent authorities, as appropriate, in their efforts to locate and recover radioactive material, including cooperating in on-site and off-site response.

## Sabotage

15. For using and storing material in secured areas assigned security level A and for transporting enhanced security packages:
- (a) the managing entity must determine whether an act of sabotage could result in unacceptable radiological consequences in the absence of physical protection or mitigation measures
  - (b) if an act of sabotage could result in unacceptable radiological consequences as determined in clause 15(a) the managing entity must:
    - (i) establish a contingency plan setting out the measures required to mitigate or minimise the radiological consequences
    - (ii) implement the measures identified in the contingency plan
    - (iii) notify the Office of Radiation Safety.



# Appendix 1: Assigning a security level for use and storage

## 1A. Secured area has no nuclear material

Follow these steps to determine the security level: A, B, C or D.

Step 1A-1 Determine all practices (from the table below) that apply to radioactive material in the secured area.

**Table 1**

Practice	Security level
Radioisotope thermoelectric generators	
Irradiators except blood irradiators	
Teletherapy	A
Fixed multibeam teletherapy (gamma knife)	
Blood irradiators	
Industrial radiography gamma radiography	B
High or medium dose rate brachytherapy	
Fixed industrial gauges with high-activity radioactive material	
Well logging gauges	C
Low dose rate brachytherapy	
Industrial gauges with only low-activity radioactive material	
Bone densitometers	
Static eliminators	
XRF devices	D
Electron capture devices	
Mossbauer spectrometry	
Positron emission tomography (PET)	

- Step 1A-2 If only one practice applies to the secured area then assign the relevant security level.
- Step 1A-3 If more than one practice applies to the secured area then assign the highest security level (A is high, D is low).
- Step 1A-4 Proceed to step 1A-5 if there is also radioactive material in the secured area that does not have a practice associated with it (eg, material in long-term storage).
- Step 1A-5 Determine the current radioactivity of each radioactive source in the secured area that is not associated with a practice.
- Step 1A-6 Calculate the A/D ratio for each of those radioactive sources by dividing its radioactivity (determined from step 1A-5) by its D-value (see Appendix 3).
- Step 1A-7 Calculate the aggregate A/D ratio for all radioactive material in the secured area that is not associated with a practice by adding the individual A/D ratios from step 1A-6.
- Step 1A-8 Assign an activity-based security level to the secured area in line with this table:

**Table 2**

Aggregate A/D ratio (x)	Security level
$x \geq 1,000$	A
$1,000 > x \geq 10$	B
$10 > x \geq 1$	C
$x < 1$	D

- Step 1A-9 Assign a final security level to the secured area that is the highest of the levels calculated in steps A-2, A-3 and A-8.

## 1B. Secured area has only nuclear material

- Step 1B-1 Determine the mass of each item of nuclear material to be used or stored in the secured area.
- Step 1B-2 Add the individual masses from step 1B-1 to obtain totals for each of:
- unirradiated plutonium
  - unirradiated uranium-235 enriched to 20% or more
  - unirradiated uranium-235 enriched to 10% or more but less than 20%
  - unirradiated uranium-235 enriched above natural but less than 10%
  - unirradiated uranium-233.

Step 1B-3 Assign security level C<sup>4</sup> to the secured area if the total mass of any type of nuclear material exceeds the levels in this table:

Nuclear material type	Mass
unirradiated plutonium	15 g
unirradiated uranium-235 enriched to 20% or more	15 g
unirradiated uranium-235 enriched to 10% or more but less than 20%	1 kg
unirradiated uranium-235 enriched above natural but less than 10%	10 kg
unirradiated uranium-233	15 g

Step 1B-4 Change the assignment from step 1B-3 to security level D if all material that exceeds the levels in the table is in a form that is no longer usable for any nuclear activity, minimises environmental dispersal and is practicably irrecoverable.

Step 1B-5 Assign security level D to the secured area if contains nuclear material but is not assigned security level C<sup>5</sup>.

## 1C. Secured area has both nuclear and non-nuclear material

Step 1C-1 Determine the security level for the secured area from the 'Secured area has no nuclear material' (Section 1A).

Step 1C-2 Determine the security level for the secured area from the 'Secured area has only nuclear material' (Section 1B).

Step 1C-3 Assign a security level to the secured area that is the higher of the two levels from steps 1C-1 and 1C-2.

---

## Examples

### Example 1

A hospital uses Ir-192 radioactive sources for high dose rate brachytherapy and keeps them in a secured room.

- The room has a single set of access controls and is therefore a secured area.

<sup>4</sup> New Zealand does not have any nuclear material that would require security levels A or B to be assigned.

<sup>5</sup> This means that secured areas that contain only natural uranium, depleted uranium and thorium will be assigned security level D.

- High dose rate brachytherapy is a practice listed in the table with an assigned security level of B
- Security level B is therefore assigned to the room irrespective of the radioactivity of the radioactive source(s).

### **Example 2**

A storage room contains a 2.8 TBq Ir-192 radioactive source with depleted uranium shielding in long term storage.

- The storage room has a single set of access controls and is, therefore, a secured area.
- Long term storage is not a practice listed in the table and therefore the security level cannot be assessed according to practice.
- Ir-192 is radioactive material but not nuclear material. Depleted uranium is nuclear material. The steps in the 'Secured area has both nuclear and non-nuclear material' section apply.
- Security level B should be assigned to the storage room for its radioactive material contents because:
  - the Ir-192 has a current radioactivity of 2.8 TBq (Step 1A-5)
  - the D-value for Ir-192 from Appendix 3 is 0.08 TBq meaning that the A/D ratio for the source is 35 (Step 1A-6)
  - this is the only radioactive source in the secured area and therefore the aggregate A/D ratio for the storage room is 35 (Step 1A-7)
  - security level B should be assigned because this exceeds 10 but is less than 1,000 (From Table 2 in 1A-8).
- Security level C should be assigned to the storage room for its nuclear material contents because:
  - depleted uranium is not listed in the table in step 1A-2
  - security level C should therefore be assigned according to step 1B-5.
- The overall security level to be assigned to the storage room is security level B because this is the higher security level calculated for each of its radioactive and nuclear contents.

# Appendix 2:

## Security level - transport

### 2A. Package contains no nuclear material

- Step 2A-1 Categorise the package as an excepted security package if the requirements for excepted packages in the IAEA Transport Regulations are met.
- Step 2A-2 Continue to step 2A-3 only if the package is not categorised as an excepted security package.
- Step 2A-3 Determine the current radioactivity of each radioactive source to be transported in the package.
- Step 2A-4 Calculate the A/D ratio for each sealed radioactive source by dividing its radioactivity (from step 2A-3) by its D-value (from Appendix 3).
- Step 2A-5 Calculate the aggregate A/D ratio for all sealed radioactive material in the package by adding the individual A/D ratios from step 2A-4.
- Step 2A-6 Calculate the A/A2 ratio for each unsealed radioactive source by dividing its radioactivity (from step 2A-3) by its A2-value (from Appendix 3).
- Step 2A-7 Calculate the aggregate A/A2 ratio for all unsealed radioactive material in the package by adding the individual A/A2 ratios from step 2A-6.
- Step 2A-8 Categorise the package as an enhanced security package if the aggregate A/D ratio exceeds 10 or the aggregate A/A2 ratio exceeds 3,000.
- Step 2A-9 Continue to step 2A-10 only if the package is not categorised as an enhanced security package.
- Step 2A-10 Categorise the package as a basic security package.

## 2B. Package only contains nuclear material

- Step 2B-1 Determine the mass of each item of nuclear material to be transported in the package.
- Step 2B-2 Add the individual masses from step 2B-1 to obtain totals for each of:
- unirradiated plutonium
  - unirradiated uranium-235 enriched to 20 percent or more
  - unirradiated uranium-235 enriched to 10 percent or more but less than 20 percent
  - unirradiated uranium-235 enriched above natural but less than 10 percent
  - unirradiated uranium-233.
- Step 2B-3 Categorise the package as an enhanced security package if the total mass of any type of nuclear material exceeds the levels in this table:

Nuclear material type	Mass
unirradiated plutonium	15 g
unirradiated uranium-235 enriched to 20% or more	15 g
unirradiated uranium-235 enriched to 10% or more but less than 20%	1 kg
unirradiated uranium-235 enriched above natural but less than 10%	10 kg
unirradiated uranium-233	15 g

- Step 2B-4 Categorise the package as a basic security package if it contains nuclear material but is not categorised as an enhanced security package<sup>6</sup>.

## 2C. Package contains both nuclear and non-nuclear material

- Step 2C-1 Determine the security classification of the package from the 'Package contains no nuclear material' (Section 2A).
- Step 2C-2 Determine the security classification of the package from the 'Package only contains nuclear material' (Section 2B).
- Step 2C-3 Categorise the package as the higher of the classifications from steps 2C-1 and 2C-2.

<sup>6</sup> This means that packages that contain only natural uranium, depleted uranium and thorium will be categorised as basic security packages.

---

## Examples

### Example 1 – Industrial radiography iridium-192 source exchange

An industrial radiography company imports a 2.8 TBq Ir-192 radioactive source for a gamma camera. This will replace an old Ir-192 that has decayed to 100 GBq and will be returned to the supplier. The transport containers are shielded with depleted uranium.

#### *Import package*

- Ir-192 is radioactive material but not nuclear material. Depleted uranium is nuclear material. The steps in the 'Package contains both nuclear and non-nuclear material' (Section 2C) apply.
- The imported package should be categorised as an enhanced security package for its radioactive material contents because:
  - the Ir-192 source has a current radioactivity of 2.8 TBq (Step 2A-3)
  - Ir-192 is sealed radioactive material meaning that steps 2A-4 and 2A-5 apply (and steps 2A-6 and A-27 don't apply)
  - the D-value for Ir-192 from Appendix 3 is 0.08 TBq meaning that the A/D ratio for the source is 35 (Step 2A-4)
  - this is the only radioactive source in the package and therefore the aggregate A/D ratio for the package remains at 35 (Step 2A-5)
  - this exceeds 10 and therefore the package is an enhanced security package (Step 2A-8).
- The imported package should be categorised as a basic security package for its nuclear material contents because:
  - depleted uranium is not listed in the table in step 2B-3
  - the package should therefore be categorised as a basic security package (Step 2B-4).
- Overall the imported package is categorised as an enhanced security package because this is the higher of the two categorisations calculated above steps 2A-8 and 2B-4.

#### *Export package*

- The exported package should be categorised as a basic security for its radioactive material contents because:
  - the Ir-192 source has a current radioactivity of 100 GBq or 0.1 TBq (Step 2A-3)
  - Ir-192 is sealed radioactive material meaning that 2A-4 and 2A-5 apply (and steps 2A-6 and 2A-7 don't apply)
  - the D-value for Ir-192 from Appendix 3 is 0.08 TBq meaning that the A/D ratio for the source is 1.25 (Step 2A-4)

- this is the only radioactive source in the package and therefore the aggregate A/D ratio for the package is 1.25 (Step 2A-5)
- this is less than 10 and therefore the package is a basic security package according to step 2A-8.
- The imported package should be categorised as a basic security package for its nuclear material contents because:
  - depleted uranium is not listed in the table in step 2B-3
  - the package should therefore be categorised as a basic security package according to step 2B-4.
- Overall the exported package is categorised as a basic security package based on the two categorisations calculated from steps 2A-8 and 2B-4 above.

### **Example 2** – Iodine-131 transport

A nuclear medicine department transports 200 MBq surplus I-131 to a veterinary clinic to treat a thyroid condition in a cat.

- The I-131 source has a current radioactivity of 200 MBq or  $2 \times 10^{-4}$  TBq (Step 2A-3).
- I-131 is unsealed radioactive material meaning that steps 2A-6 and 2A-7 apply (and steps 2A-4 and 2A-5 don't apply).
- The A2 value for I-131 from Appendix 3 is 0.7 TBq meaning that the A/A2 ratio for the source is  $2.9 \times 10^{-4}$ .
- This is less than 3,000 and, therefore, the package is a basic security package according to step 2A-8.

### **Example 3** – Nuclear density meter transported for field operations

A civil engineering company transports a nuclear density meter to perform field work. The meter contains two sealed radioactive sources – Am-241 with a current activity of 1.48 GBq (0.00148 TBq) and Cs-137 with a current activity of 0.37 GBq (0.00037 TBq).

- Both sources are sealed radioactive sources meaning that steps 2A-4 and 2A-5 apply (and steps 2A-6 and 2A-7 do not apply).
- The A/D ratios of these two sources are:
  - Am-241 –  $0.00148 \div 0.06 = 0.0247$
  - Cs-137 –  $0.00037 \div 0.1 = 0.0037$ .
- The aggregate A/D ratio for the package is 0.0284 (Step 2A-7).
- This is less than 10 and, therefore, the package is a basic security package according to step 2A-8.



# Appendix 3:

## D and A2-values

Radionuclide	D-value <sup>7</sup> (TBq)	A2-value <sup>8</sup> (TBq)
Am-241	6.E-02	1.E-03
C-14	5.E+01	3.E+00
Cf-252	2.E-02	6.E-03
Co-57	7.E-01	1.E+01
Co-60	3.E-02	4.E-01
Cs-137	1.E-01	6.E-01
F-18	6.E-02	6.E-01
Gd-153	1.E+00	9.E+00
Ge-68	7.E-01	5.E-01
H-3	2.E+03	4.E+01
I-131	2.E-01	7.E-01
Ir-192	8.E-02	6.E-01
Lu-177	2.E+00	7.E-01
Mo-99	3.E-01	6.E-01
Pm-147	4.E+01	2.E+00
Pu-238	6.E-02	1.E-03
Pu-239/Be	6.E-02	1.E-03
Ra-226	4.E-02	3.E-03
Se-75	2.E-01	3.E+00
Sr-90 (Y-90)	1.E+00	3.E-01
Tc-99 <sup>m</sup>	7.E-01	4.E+00
Tl-204	2.E+01	7.E-01

<sup>7</sup> D-values for radionuclides not listed in the table are available at [www-pub.iaea.org/MTCD/Publications/PDF/EPR\\_D\\_web.pdf](http://www-pub.iaea.org/MTCD/Publications/PDF/EPR_D_web.pdf) or from the Office of Radiation Safety.

<sup>8</sup> A2-values for radionuclides not listed in the table are available at: [www-pub.iaea.org/MTCD/Publications/PDF/PUB1798\\_web.pdf](http://www-pub.iaea.org/MTCD/Publications/PDF/PUB1798_web.pdf) (Table 2) or from the Office of Radiation Safety.

# Appendix 4:

## Security goals

Activity	Security goal
Use or storage of radioactive material in secured areas assigned security level A.	Provide a high level of protection of the material against unauthorised removal
Use or storage of radioactive material in secured areas assigned security level B.	Provide an intermediate level of protection of the material against unauthorised removal
Use or storage of radioactive material in secured areas assigned security level C or D.	Provide a fundamental level of protection of the material against unauthorised removal
Transport of radioactive material in enhanced security packages.	Provide a high level of protection of the material against unauthorised removal
Transport of radioactive material in basic security packages and excepted security packages.	Provide a fundamental level of protection of the material against unauthorised removal

# Appendix 5:

## Security plans

This appendix sets out the requirements for security plans as required by clauses 3(f) and 6(b). Requirements differ depending on whether radioactive material is for use and storage or for transport. If material is to be transported as well as being used or stored, then the security plan must satisfy the requirements in both sections of this appendix.

### Use and storage

#### Introduction

1. Objectives of the plan – such as documenting the operation of the security system and security management measures to demonstrate compliance with this code of practice
2. Scope – brief description of the scope of the plan including links to relevant documents
3. Preparation and updating – the process for developing, updating and approving the plan

#### Facility

1. Description and location of radioactive material
2. Assessed security levels assigned to each secured area
3. Description of the physical features of the facility

#### Security management

1. Description of the measures in place to meet the requirements of clauses 1 to 4 of this code of practice, including:
  - (a) roles and responsibilities and details of the appointed radiation security officer
  - (b) training and qualifications
  - (c) access authorisation
  - (d) trustworthiness and reliability
  - (e) information protection
  - (f) maintenance programme
  - (g) budget and resource planning
  - (h) evaluation for compliance and effectiveness

## Security system

1. Procedures to obtain threat information
2. If applicable, how the threat information is received and shared with personnel who have a need to know
3. Process and methodology used to evaluate the security system
4. How the security system has been designed to provide the level of protection required
5. Physical measures for controlling access
6. Detection, delay and alarm assessment measures

## Security procedures

1. Written security procedures for personnel who implement and maintain them

## Response

1. Description of response measures for all security events

## Transport

### Introduction

1. Objectives of the plan – such as documenting the operation of the security system and security management measures to demonstrate compliance with this code of practice
2. Scope – brief description of the scope of the plan including links to relevant documents
3. Preparation and updating – the process for developing, updating and approving the plan

### Shipment details

1. Description of radioactive material
2. Mode(s) of transport

### Administrative requirements

1. Policies and procedures
2. Vulnerability and threat assessment
3. Testing and evaluating the security plan
4. Transport security verification
5. Notification of relevant agencies

## Personnel qualifications

1. Trustworthiness
2. Training

## Responsibilities

1. Organisational structure
2. Allocation and transfer of responsibilities

## Information management

1. Information security
2. Records retention

## Transport security measures

1. Routes
2. Transport security system (conveyance, operations command and control, physical protection measures, communication and positional tracking for normal operations, maintenance and testing of systems and equipment)

## Emergency response

1. Emergency and contingency response
2. Communications during incidents
3. Reporting of threats and incidents

# Appendix 6: Training

	Security Officer				Operator			
	SLA	SLB	SLC	Tspt	SLA	SLB	SLC	Tspt
Radioactive material security threats and risks	h	h	m	l	m	m	l	l
IAEA radioactive material security series publications	l	l	l	l	x	x	x	x
Radiation basics	m	m	m	m	m	m	l	l
Consequences of exposure to radiation	m	m	l	l	m	m	l	l
Physical protection	h	h	m	m	m	m	l	l
Categorisation of radioactive sources	m	m	l	l	m	m	l	l
Radioactive sources and their application	l	l	l	l	l	l	l	l
Transport security	x	x	x	h	x	x	x	m
Preventive and protective measures against insider threats	h	x	x	m	m	x	x	l
Material out of regulatory control	h	m	m	m	m	m	l	l
Information security	h	m	m	l	m	m	l	l
Security plans	m	m	m	m	l	l	l	l

## Abbreviations used in this appendix

### Parties

SLA – secured areas assigned security level A

SLB – secured areas assigned security level B

SLC – secured areas assigned security level C

Tspt – enhanced security transport packages

### Level of knowledge

x – no requirement

l – low level of knowledge (general awareness and understanding of principles)

m – medium level of knowledge (basic understanding of the topic sufficient to influence practices undertaken)

h – high level of knowledge (detailed knowledge and understanding sufficient to be able to educate others)